Narušavanje privatnosti pojedinca u Iot okruženju

Radovanović, Slavko

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Slavko Radovanović

NARUŠAVANJE PRIVATNOSTI POJEDINCA U IOT OKRUŽENJU

ZAVRŠNI RAD

Varaždin, 2018.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Slavko Radovanović

Matični broj: 40079/11–IZV

Studij: Poslovni sustavi

NARUŠAVANJE PRIVATNOSTI POJEDINCA U IOT OKRUŽENJU

ZAVRŠNI RAD

Mentorica:

Doc. dr. sc. Renata Mekovec

Varaždin, rujan 2018.

Slavko Radovanović

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

_____

Sažetak

Internet stvari je relativno novi pojam u današnjem svijetu iako se razvija već dugi niz godina. Razlog tome je napredak tehnologija i sustava koji omogućuju takva okruženja. U ovom radu naglasak će biti na moguće propuste u sigurnosti takvih okruženja koji mogu značiti narušavanje privatnosti pojedinaca koji se koriste tim sustavima. Kroz nekoliko primjera korištenja Interneta stvari u različitim sferama života ljudi pokušat ću prikazati s kojima problemima se suočavaju ljudi koji isti razvijaju. Osim teorijskog dijela provest ću anketu da bih dobio uvid u razmišljanje potencijalnih korisnika sustava Interneta stvari, koliko ih je upoznato s takvim sustavima, smatraju li da je sigurnost na zadovoljavajućoj razini i da li bi pristali živjeti u pametnoj kući.

Ključne riječi: Internet stvari; Internet; privatnost; sigurnost; stvari; komunikacija;

Sadržaj

1. Uvod

Internet stvari (eng. Internet of Things – IoT) je pojam koji obuhvaća sve stvari koje su spojene na Internet i imaju mogućnost međusobnog komuniciranja. Kao ideja postoji od razvoja računala i neprestano se razvija. Krajnji cilj kojeg bi Internet stvari trebao ostvariti je ostvarivanje utopije na svijetu, gdje se čovjek ne mora zamarati sitnicama nego ima uređaje koji obavljaju većinu stvari umjesto njega. Ta ideja se prvo pojavljivala kao zamišljanje budućnosti u znanstveno-fantastičnim djelima, poglavito u filmovima i serijama. Većina inovacija je imala začetke u znanstvenoj-fantastici, npr. podmornice su nastale na ideji iz knjige Julesa Verna *Dvadeset milja pod morem*, prvi bežični mobitel koji je Motorola napravila 1973. godine je nastao iz ideje komunikatora iz serijala *Zvjezdane staze*, jedna od prvih ideja koja je potakla razvoj Interneta stvari je ideja obiteljskog doma u kojem uređaji većinu stvari odvijaju bez ili s minimalnim učešćem ljudi, takozvana *Pametna kuća*, a ideja je preuzeta iz filma *Povratak u budućnost 2*.

Svakog dana sve se više uređaja povezuje u Internet stvari, sve više kontrole se prepušta uređajima radi efikasnijeg korištenja resursa i smanjenja troškova. No da bi Internet stvari funkcionirao potrebni su mu podaci, a ti podaci mogu biti osjetljive prirode, poput OIB-a korisnika, no osim njih Internet stvari stvara gomilu podataka koje sprema i dijeli preko internetske veze s drugim uređajima ili sa udaljenom bazom podataka. Zbog toga se velika važnost pridodaje sigurnosti sustava Interneta stvari. Nitko ne želi da njegovi ili njezini osobni podaci postanu javni. Tu se već nazire prva velika prepreka i izazov za Internet stvari, a to je povjerenje potencijalnih klijenata. Međutim potencijalne koristi koje Internet stvari pruža su gotovo neograničene, sustavi koji će se razviti promijenit će način na koji živimo i način na koji radimo, uštedit će nam vrijeme obavljanjem osnovnih poslova umjesto nas pritom štedeći energiju i resurse i omogućit razvoj još kompleksnijih sustava. Glavna tehnologija koja će najviše utjecati na razvoj novih sustava Interneta stvari je golema količina podataka (eng. Big Data). Stvari će pomoću senzora prikupljati ogromnu količinu podataka te ih cijelo vrijeme procesuirati i donositi nove načine upravljanja svijeta u kojem živimo.

2. Internet stvari

Postoji mnogo definicija Interneta stvari. Prema IERC-u (eng. *European Research Cluster on the Internet of Things*) Internet stvari je integralan dio budućeg Interneta i može se definirati kao dinamička globalna mrežna infrastruktura s mogućnostima samokonfiguracije bazirane na standardnim i interoperabilnim komunikacijskim protokolima gdje fizičke i virtualne 'stvari' imaju identitete, fizičke atribute i virtualne osobnosti te koriste inteligentna sučelja i neprekidno su uključena u informacijsku mrežu [1]. Nadalje IDC (eng. *International Data Corporation*) definira Internet stvari kao mrežu više mreža koje imaju jedinstvene identifikacijske 'stvari' koje komuniciraju bez ljudske interakcije koristeći IP konektivnost, lokalnu ili globalnu. S obzirom da je ta komunikacija između 'stvari' konstantna, Internet stvari ostvaruje koncept neprestane povezanosti za poduzeća, vlade i korisnike te omogućuje lakše upravljanje, praćenje i vođenje analitike [2]. Internet stvari spaja dva koncepta, prvi je da se uređaji mogu povezati u mrežu bilo kad i bilo gdje, a drugi koncept je neprestano procesuiranje informacija. Misao vodilja razvoja Interneta stvari je citat Marka Weisera iz članka „Računalo za 21. stoljeće“ (eng. *The Computer for the 21st Century*): „najsmislenije tehnologije su one koje nestanu“ [3]. Želja je da uređaji koji omogućuju Internet stvari postanu 'nevidljivi' korisnicima, odnosno da ljudi ne obraćaju pažnju na njih kao na nešto posebno nego kao na obično oruđe kojim se koriste, kao što su na primjer naočale, čovjek ne gleda u naočale, nego pomoću naočala gleda u svijet. Internet stvari teži komunikaciji između uređaja koji bi razmjenjivali podatke, a u pozadini bi sustav procesuirao sve prikupljene podatke u svrhu raznih poboljšanja koja bi pogodovala korisnicima, kao što je ušteda energije ili povećanje udobnosti[4].

Internet stvari je sustav međusobno povezanih stvari kojima su dodijeljeni jedinstveni identiteti unutar strukture koja je slična Internetu. Unutar te strukture svakodnevne stvari i objekti imaju svoju virtualnu sliku te mogu međusobno komunicirati i prenositi podatke, a da u tom komuniciranju i prijenosu podataka sudjelovanje čovjeka nije nužno[5]. Internet stvari daje mogućnost automatiziranja velike većine poslova i svakodnevnih aktivnosti, a stvar u Internetu stvari može biti doslovno svaki objekt u stvarnom životu, od osobnog računala, preko pametnih telefona, automobila, strojeva, kućanskih aparata pa do vrata, prozora, stolica i svega ostaloga što čovjek može zamisliti. Frazu Internet stvari skovao je Kevin Ashton još 1999. kao naslov prezentacije dok je radio za Procter i Gamble. U toj prezentaciji on opisuje mrežu koja spaja objekte iz svakodnevnog života direktno na Internet. U članku „Ta 'Internet stvari' stvar“ (eng. *That 'Internet of Things' Thing*) iz 2009. Ashton navodi da su računala, s njima i Internet, u potpunosti ovisna o ljudima za prikupljanje informacija,

odnosno skoro sve podatke dostupne na Internetu su ljudi prvo morali natipkati, snimiti mikrofonom, snimiti kamerom ili skenirati barkod[6].

Naravno, postavlja se pitanje koja je svrha takvog povezivanja svih stvari? Hoće li povezivanje stvari omogućiti brže prikupljanje informacija? Mogu li stvari prikupiti više informacija nego ljudi? Hoće li prikupljanje biti točnije i preciznije? Prema Ashtonu ljudi imaju problem što su im vrijeme, pozornost i preciznost ograničeni[6]. Stvarima treba biti omogućeno da vide, čuju i osjete miris svijeta oko sebe i da te podatke prenose na mrežu i upravo u tom smjeru se razvija Internet stvari. Tako prikupljene informacije bi nam omogućile da pratimo sve što se događa, da smanjimo prekomjernu potrošnju resursa i troškove koji se mogu izbjeći.

Umreženi sustavi, odnosno Internet stvari već postoje. S obzirom da ti sustavi obavljaju određene zadatke koji se čine komplicirano, dodijeljen im je prefiks 'pametan'. U nastavku su opisani neki primjeri kako se Internet stvari može iskoristiti u osobne svrhe, industrijske i političke. Tako se i IoT sustavi mogu podijeliti na tri kategorije. Prvi su sustavi kojima se koriste individualni građani, druga kategorija su sustavi koje koriste poduzeća i industrije, a treća su sustavi koje koriste određene grupe građana, poput stanovnika jednog grada. Internet stvari može pogodovati svim kategorijama iz nekoliko razloga. Individualni građani će prihvatiti Internet stvari jer će im pružiti veći osjećaj sigurnosti njih samih i njihovih obitelji, njihovih osobnih stvari, pružiti će im veći osjećaj lagodnosti jer će lakše izvršavati neke svakodnevne zadatke, poboljšati će im način života i smanjiti troškove. Poduzeća će povećati produktivnost, moći će cijelo vrijeme pratiti stanje na tržištu te će smanjiti troškove vođenja posla. Grupe građana, na primjer u gradu će se poboljšati opća sigurnost, biti će veća zaštita okoliša i efikasnije će se trošiti energija[7]. Prepuštanjem kontrole uređajima nad određenim akcijama pridodala im se riječ 'pametno', poput mobitela. Isti trend je i kod prvih sustava Interneta stvari, međutim možda bi primjerenije bilo reći da su ti sustavi inteligentni. No prije primjera opisat ću što je potrebno da se ostvari sustav Interneta stvari.

2.1. Ostvarivanje Interneta stvari

Jedna od najbitnijih karakteristika Interneta stvari je da su sve stvari povezane u jedan sustav, odnosno sve komuniciraju međusobno, a to predstavlja problem jer sve stvari moraju biti sukladne. Zbog tog razloga se nastoji napraviti standard kojeg će se svi proizvođači morati pridržavati da se uopće mogao ostvariti takav sustav. Nakon što je sukladnost postignuta Internet stvari mora posjedovati slijedeće komponente[8]:

- Modul za komuniciranje sa lokalnim IoT uređajima koji je zadužen da šalje prikupljene podatke na server za obradu i pohranjivanje

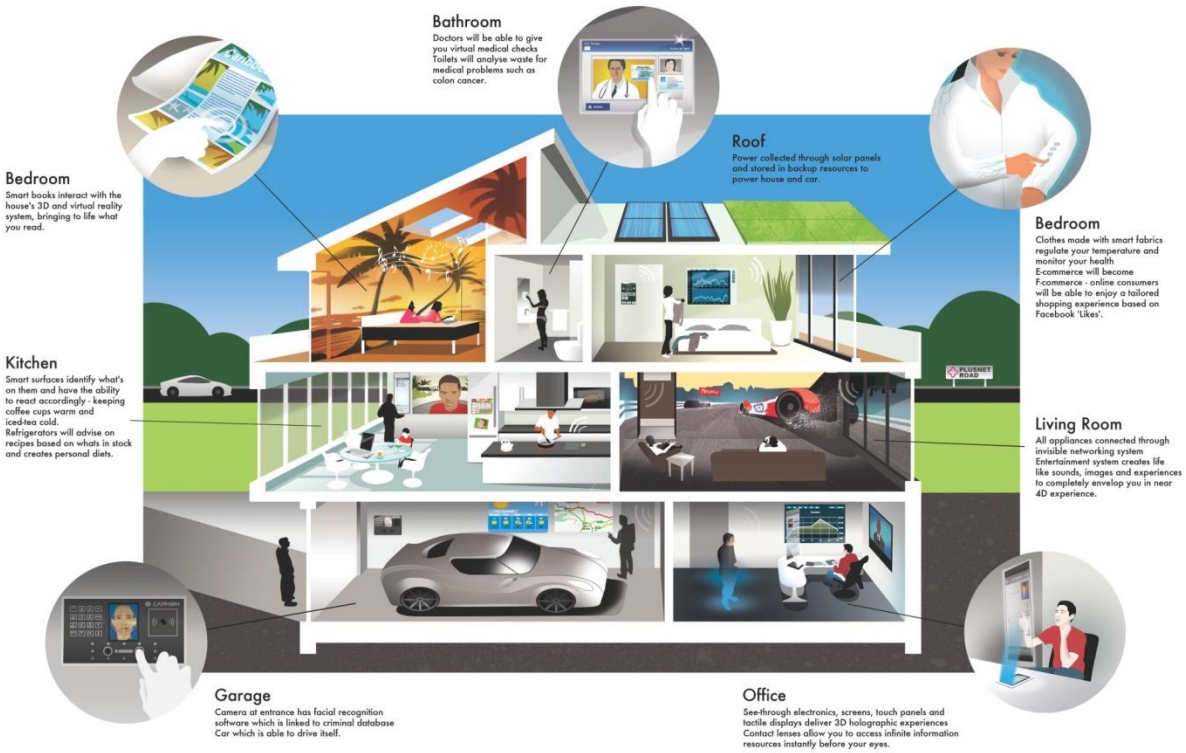
- Modul za lokalnu analizu i obradu podataka koje su prikupile 'stvari'
- Modul za interakciju sa udaljenim IoT uređajima preko Interneta koji je zadužen da šalje prikupljene podatke na server za obradu i pohranjivanje
- Modul za specijalnu obradu i analizu podataka koji se nalazi na serveru
- Modul za integriranje informacija iz IoT-a u poslovne procese poduzeća
- Korisničko sučelje

Internet stvari je evolucija Interneta te bi stoga morao preuzeti njegove najbolje značajke, a najbolja stvar Interneta je što je otvoren i dostupan svima. Kako bi Internet stvari preuzeo tu otvorenost važno je da aplikacije za razvoj sučelja (eng. *Application Programming Interface*, kraće API) budu dostupni svima. To bi omogućilo brži razvoj i dodavanje vrijednosti Internetu stvari, a vjerojatno bi se pojavile i nove mogućnosti unutar takvih sustava. Modul koji bi sigurno profitirao od otvorenih API-ja je modul za obradu i analizu podataka na serveru jer bi se omogućilo developerima da iskoriste maksimum od cijelog sustava[8].

2.2. Pametna kuća

Povezivanje obiteljskog doma u Internet stvari omogućuje upravljanje i nadzor nad vlastitom kućom, uređajima te stvarima koje su povezane bez obzira gdje se vlasnik nalazi u svijetu te može doprinijeti smanjenju troškova. Termostat povezan u Internet stvari može sam sniziti temperaturu u kući ukoliko se nitko ne nalazi istoj ili ako vremenska prognoza pokazuje visoke vrućine tog dana. Vlasnik može provjeriti da li su svi kućanski uređaji isključeni. Perilica za rublje će se sama uključiti kada je jeftinija struja te će sama odabrati optimalni program za pranje. Ako nitko ne boravi u određenoj prostoriji svjetla se sama ugase. U članku „Kako ljudi stvarno koriste Internet stvari“ (eng. *How People Are Actually Using the Internet of Things*) kojeg su napisali H.James Wilson, Baiju Shah i Brian Whipple, opisuje to povezivanje[9]. Kad vlasnik sa osobnim automobilom priđe garaži sa pametnim vratima, ona se aktiviraju i krenu otvarati te šalju signal pametnoj bravi koja otključava kuću, zatim signal ide prema svjetlima da se upale ukoliko je noćno doba, u isto vrijeme signal ide i do termostata da upali zagrijavanje ili hlađenje kuće, zavisno o trenutnoj temperaturi u kući.

Osim automatizacije, Internet stvari omogućava i zaštitu obiteljskog doma ugradnjom kamera koje se aktiviraju senzorima za pokret i pametnim prozorima i vratima koje jedino vlasnik preko aplikacije ili lozinke, odnosno skenera na bravi može otključati i otvoriti. Kamera snima video te ga šalje korisniku da provjeri što se dogodilo da je aktiviralo senzor. Na slici 1 vidimo prikaz kako se zamišlja da će domovi izgledati u budućnosti u sklopu Interneta stvari.



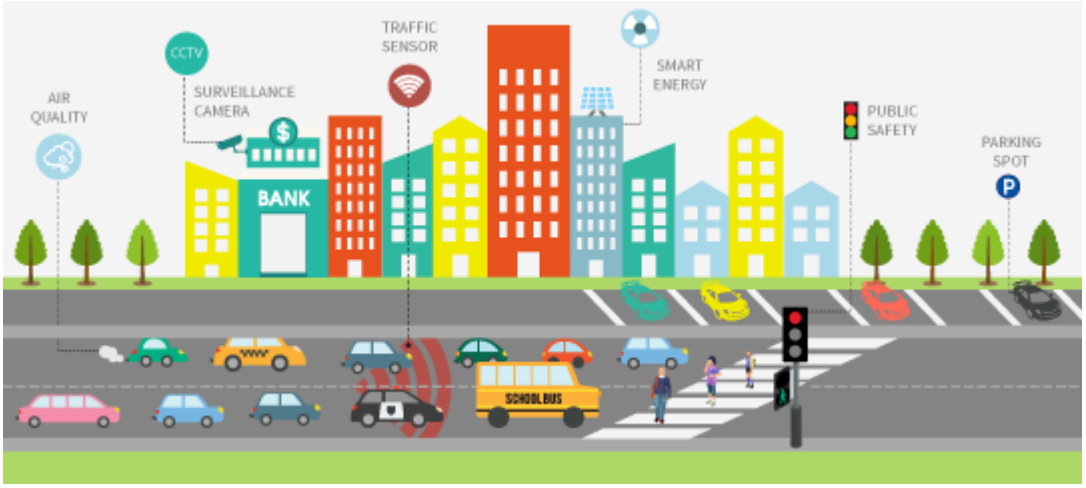
Slika 1: Pametna kuća (izvor: Smart Home Pensacola)

Pametne kuće koje se trenutno nude na tržištu se baziraju na tome da opskrbe domove tehnologijom koja će omogućiti korisniku potpunu kontrolu nad svim aparatima koristeći jedan uređaj, pametni telefon. Glavni aspekti koje proizvođači žele poboljšati na ovaj način su kontrola potrošnje energije, udobnost, pristupačnost i sigurnost. Postoje i pametne zgrade, koje su isto tako pametne kuće, ali na višoj razini. Kod njih se javljaju dodatni problemi, trebaju više informacija za funkcioniranje, poput tko je vlasnik stana, tko sve živi u stanu, ako ima više vlasnika u jednoj zgradi, pristaju li svi na jednaku tehnologiju, ukoliko je riječ o poslovnim zgradama postoji problem privatnosti jer više korisnika dijeli isti ured pa uređaj prikuplja podatke od svih njih[7]. Pametne kuće se mogu integrirati i u veći sustav Interneta stvari, pametni grad.

2.3. Pametni grad

Jedna primjena Interneta stvari bi bila povezivanje grada. Više od pola ukupnog svjetskog stanovništva živi u gradovima, a u Europi je ta brojka blizu 80% populacije. Toliko velik broj ljudi stvara problem gradskoj upravi, a jedno od mogućih rješenja tog problema je Internet stvari. Većina gradova ima problem s parkirnim mjestima, a povezivanjem svih parkirnih mjesta u Internet stvari, u stvarnom vremenu bi svaki građanin i posjetitelj grada

mogao dobiti informaciju gdje se može parkirati zajedno sa GPS navođenjem do najbližeg slobodnog parkirnog mjesta. Nadalje, gužve u prometu bi se mogle gotovo posve ukloniti tako što bi se vozačima koji idu prema gužvama slala upozorenja i predlagale alternativne rute. Odvoz smeća bi se mogao optimizirati, ne bi bilo potrebno jednom tjedno slati kamion na istu rutu ukoliko kontejneri nisu puni, sustav bi sam slagao rute vozačima i slao im navigaciju kad god bude potreban odvoz. Osvjetljenje u gradu bi se prilagođavalo vremenskim uvjetima. Gradske vlasti bi imale mapu sa razinama buke u cijelom gradu te bi mogli pravovremeno reagirati na remećenje javnog reda ukoliko razine buke krenu naglo skakati.

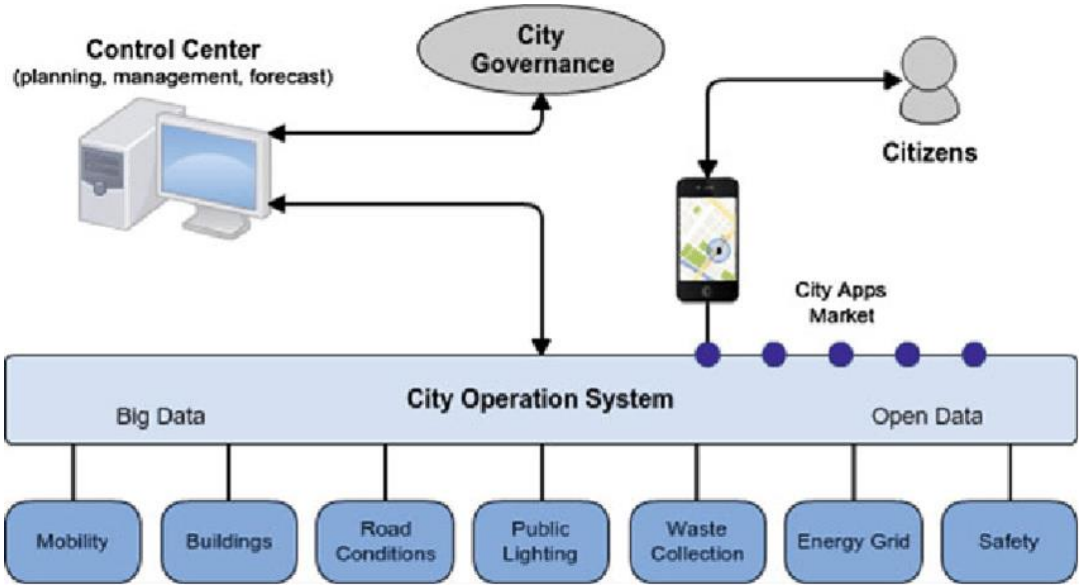


Slika 2: Pametni grad (izvor: Carlos Hernandez, 2016.)

Za pametni grad se može reći da je integracija tehnologije u strategijski pristup za održivost, dobrobit građana i ekonomski razvoj. Da bi se ostvario pametni grad nekoliko velikih sustava mora raditi skupa te stoga pametni grad se naziva i sustav sustava. Sustav koji omogućava upravljanje pametnim gradom mora biti horizontalan i interoperabilan, a to znači da pristup sustavu trebaju imati svi, međutim ne mogu svi pristupiti svim podacima. Ujedno se mora omogućiti da svi koji pristupaju sustavu mogu generirati novi sadržaj[8]. Na slici 3 je prikaz horizontalnog sustava.

Mnogi veliki gradovi uvode sustave Interneta stvari s ciljem poboljšanja života građana i čuvanju okoliša. Brian Buntz je izdvojio pet gradova koji su najviše uložili u takav sustav u članku „5 Najpametnijih gradova na svijetu“ (eng. *The World's 5 Smartest Cities*) iz 2016. godine. Na prvom mjestu njegove liste se nalazi Singapur. Republika Singapur je krajem 2014. započela program da postane prva pametna nacija. U gradu su instalirali golemi broj senzora i kamera te prate sve što se događa u gradu. Napravili su softver 'Virtualni Singapur' (eng. *Virtual Singapore*) koji koristi gomilu podataka koje prikupljaju svi senzori i kamere da bi stvorili dinamički 3D model grada. Taj model koriste planeri grada za

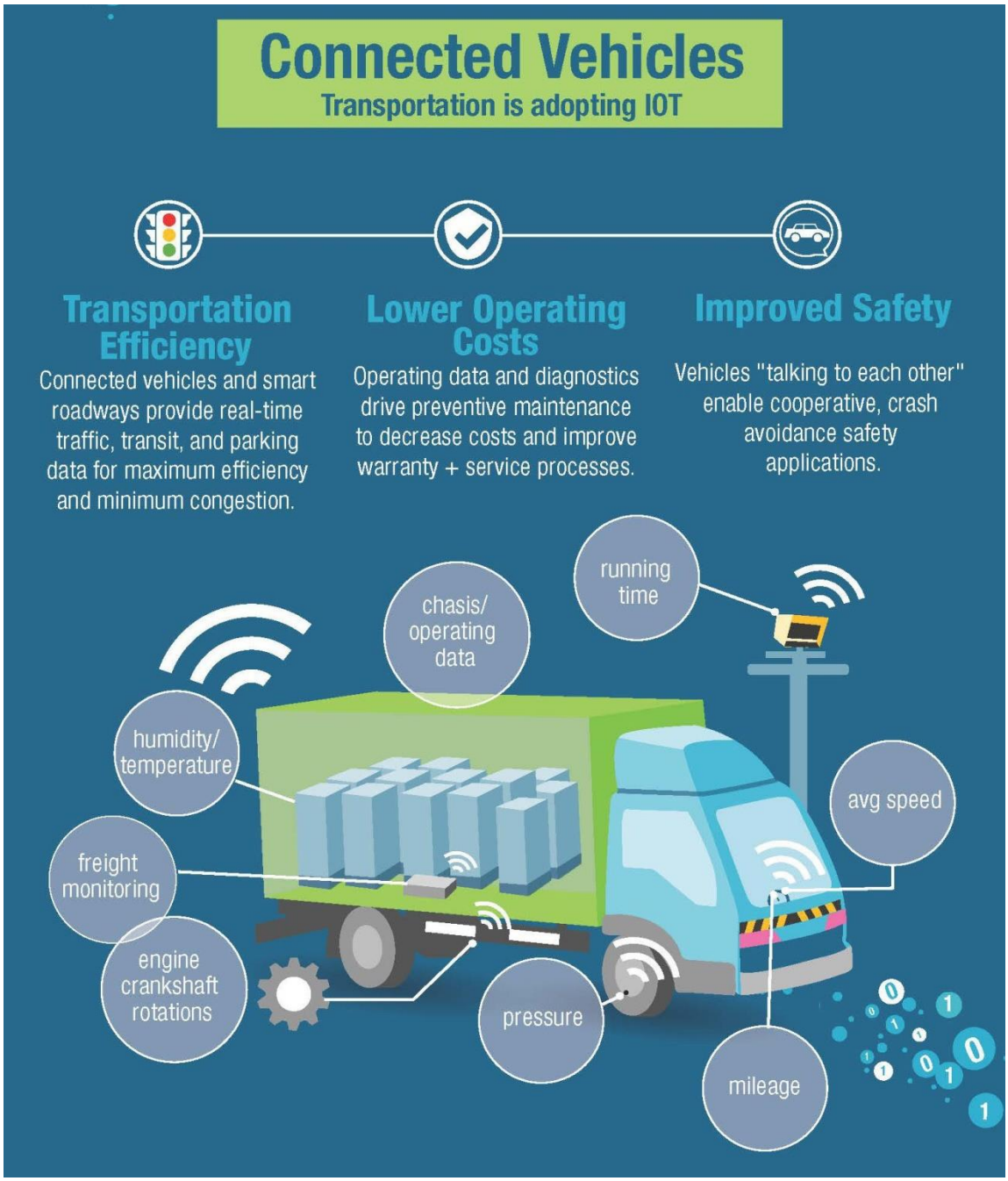
obavljanje virtualnih testova, poput evakuacije određenog dijela grada zbog uzbune. U top 5 gradova još su ušli Barcelona, London, San Francisco i Oslo[10].



Slika 3: Eko –sustav pametnog grada (izvor: Leonardo A Amaral i dr, 2017.)

2.4. Pametni transport

Nadalje, povezivanje transporta i logistike u Internet stvari bi donio niz poboljšanja u njihovo poslovanje. Vlasnici bi u svakom trenutku znali koliko robe prevoze, gdje se točno ta roba nalazi i u kakvom je stanju. Ukoliko skladište u koje je roba spremljena nije prigodno za skladištenje te robe, vlasnici bi dobili upozorenje. Kvaliteta transporta bi se povećala jer bi se svaki dio rute bio pod nadzorom i svako otvaranje transportnih kontejnera bilježilo te bi tako i zaštita robe bila veća. Na slici 4 vidimo 3 velike prednosti koje Internet stvari donosi u transport. Prva je optimiziranje ruta koje vozač treba prijeći. Druga je snižavanje troškova održavanja prijevoznih vozila, a to bi se postiglo konstantnim motrenjem dijagnostike vozila čime bi se mogla smanjiti cijena servisa istog. Zadnja velika prednost se tiče vozača, a to je sigurnost u prometu. Vozila koja komuniciraju bi mogla spriječiti potencijalne sudare. Nadalje podaci o načinu vožnje bi se stalno slali u poduzeće te ukoliko se otkrije da vozač počinje krivudati, ubrzavati ili raditi nagle pokrete, nadređeni bi dobili obavijest i mogli bi kontaktirati vozača te mu narediti da se isključi iz prometa i odmori neko vrijeme s obzirom da su to sve znaci umora od vožnje.



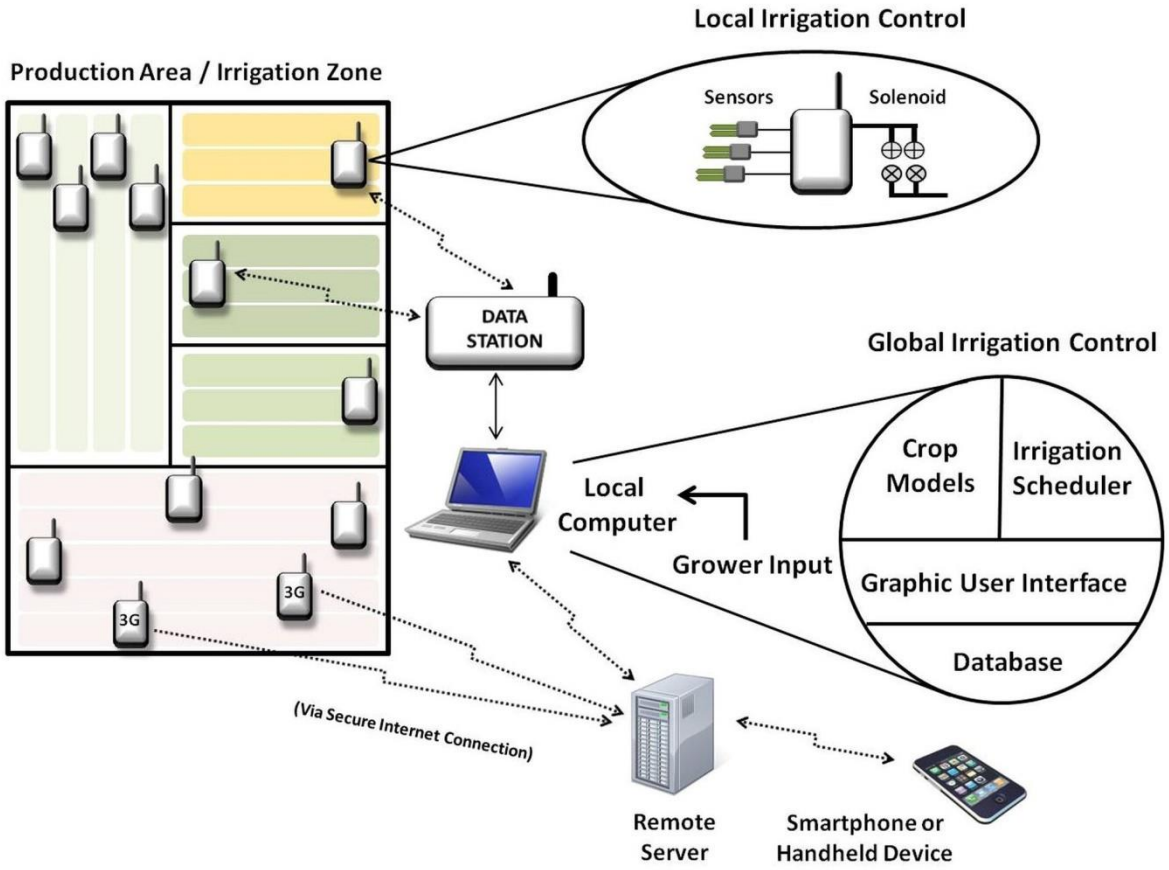
Slika 4: IoT u transportu (izvor: Yash Mehta, 2015)

Primjer Interneta stvari u transportu je poduzeće VIA koje nudi ugradnju sustava u prijevozna vozila. Glavne aplikacije koje izdvajaju su[10]:

- Prikupljanje podataka
- Analiza podataka
- Nadgledanje i kontrola
- Informacije i zabava (vozačima i putnicima)
- Video nadzor u 360 stupnjeva

2.5. Pametne farme

Uzgoj životinja na farmama se također može povezati. Kontroliranjem uvjeta u kojima biljke rastu dobili bi najveću moguću žetvu. Osim kontroliranja biljaka, mogli bi kontrolirati i uvjete u kojima mladunci životinja rastu i razvijaju se. Automatsko kontroliranje tih uvjeta osigurava zdravlje i preživljavanje istih. Lociranje i identifikacija životinja koje se puštaju na ispašu na otvorene pašnjake. Motrenje ventilacije, kvalitete zraka i toksičnih plinova u zgradama gdje životinje obitavaju bi povećalo kvalitetu konačnih proizvoda na tim farmama[7].

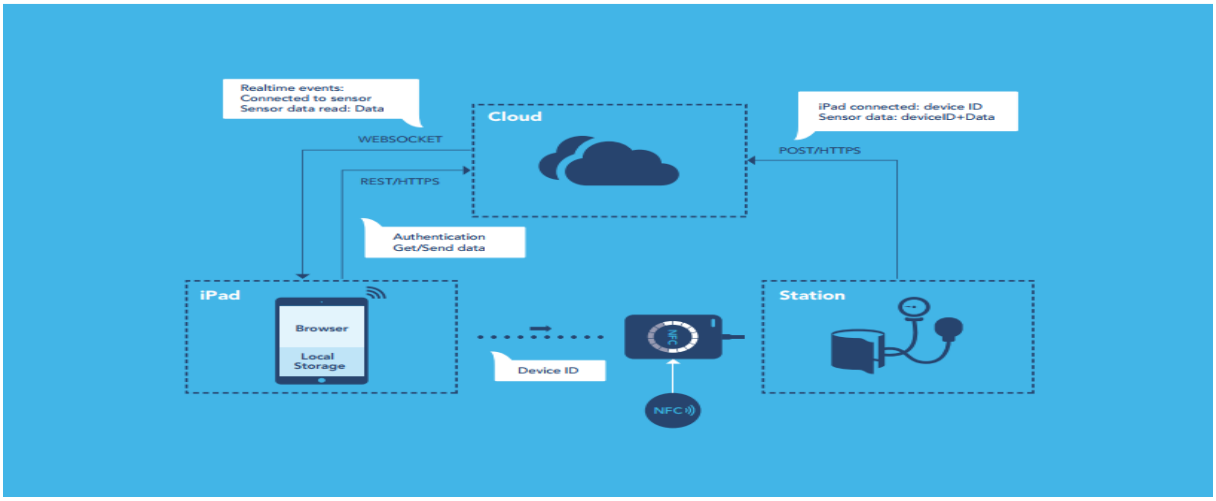


Slika 5: Pametna farma (izvor: Smart Farms Home)

Pametna farma (eng. *Smart Farms*) već postoji, na slici 5 vidimo kako su senzori povezani sa serverom. Oni navode tri faktora koja ostvaruju, a to su štednja vode, povećanje efektivnosti i smanjenje utjecaja na okoliš[12].

2.6. Pametno zdravstvo

Umrežavanje zdravstva u Internet stvari bi ubrzalo pružanje pomoći onima kojima je pomoć potrebna. Konstantni nadzor pacijenata bi imao veliki utjecaj na smanjenje smrtno stradalih osoba od bolesti i uzroka koji bi se mogli i predvidjeti, kao što je srčani udar. Redovna kontrola krvnog tlaka i kontrola pulsa putem uređaja koji bi to sam određivao te automatska obavijest najbližem liječniku u slučaju prevelikih odstupanja istih od normalnih vrijednosti bi dovela do slanja hitne medicinske pomoći unesrećenoj osobi s tim da bi uređaj koji kontrolira krvi tlak i puls imao ugrađenu uslugu GPS lokacije, koja bi se također proslijedila hitnoj pomoći. Tvrtka Omron Healthcare je već napravila sat koji očitava krvni tlak sa zgloba ruke i šalje podatke na mobilni uređaj preko bluetooth veze. Osim pružanja pomoći povezivanje u Internet stvari bi imalo i drugih posljedica za zdravstvo, kao što je produžavanje recepata pacijentima bez da dolaze na pregled ili povećanje efikasnosti u bolnicama prilikom različitih pregleda. U analizi slučaja (eng. Case study) Office Practicum koji je provela tvrtka Macadamiam prikazan je primjer povećanja efikasnosti rada u bolnicama. Prilikom testiranja pacijenata, medicinsko osoblje premješta pacijente iz sobe u sobu da bi mogli pristupiti uređajima za testiranje. Nakon svakog testiranja rezultati se zapisuju u bilješke, a te bilješke medicinske sestre nose do centraliziranih terminala gdje ih unose u zdravstveni karton pacijenta, no prije svakog unosa medicinske sestre se moraju prijaviti u sustav. Zapisivanje bilješki, nošenje bilješki te prijavljivanje oduzimaju mnogo vremena koje bi se moglo kvalitetnije utrošiti. Koncept rješenja je jednostavan, infracrveni identifikacijski broj (eng *RFID tag*) koji se nalazi u Appleovom iPadu i NFC senzor koji se nalazi u uređajima za testiranje. Podaci bi se slali automatski na server i zapisivali u zdravstveni karton pacijenta bez potrebe da medicinska sestra autorizira prijenos[13].



Slika 6: Dijagram Case Study-a (izvor: Macadamiam Case Study)

2.7. Budućnost Interneta stvari

Internet stvari više nije daleka budućnost. Svakodnevno se sve više stvari umrežava u IoT. Procjenjuje se da će do 2020. između 20 i 50 milijardi stvari biti umreženo u Internet stvari. Google, kao jedan od velikih igrača mobilnog Interneta, već je uložio u IoT kupovinom Nest Labs-a za 3,2 milijarde dolara[9]. Nest Labs je poduzeće koje se bavi automatizacijom domaćinstava. Dosad su izumili pametni termostat Nest Learning Thermostat 2011., pametni detektor dima i ugljičnog monoksida, Nest Protect 2013. godine i Nest Cam Indoor, pametna kamera koja snima unutrašnjost kuće. Pametni termostat je isprogramiran da sam zapamti kakvu temperaturu korisnik želi, sam se ugasi kad nikoga nema u kući ili stanu i može biti kontroliran preko WiFi mreže. Osim kontroliranja i podešavanja postavki i rasporeda, korisnik može vidjeti koliko energije troši. Pametni detektor dima, Nest Protect, ima ugrađen ljudski glas te informira korisnika ukoliko količina štetnih plinova postane previsoka u prostoriji. Osim upozorenja, detektor kaže korisniku u kojoj sobi u kući ili stanu je detektiran dim ili ugljični monoksid, a dovoljan je pokret ruke da ga se utiša. Pametna kamera, Nest Cam Indoor, daje korisniku mogućnost da u svakom trenutku pogleda što se događa u njegovom domu, s tim da se kamera može okrenuti u svim smjerovima jednostavnim klikom na pametnom telefonu. Osim prijenosa slike uživo, Nest Cam Indoor pruža mogućnost prijenosa zvuka u oba smjera, s tim da ignorira pozadinsku buku poput prometa, ali će upozoriti korisnika ukoliko čuje sudar, jak udarac ili nečiji glas. Pametna kamera cijelo vrijeme promatra prostoriju i ukoliko uoči aktivnost šalje upozorenje korisniku na aplikaciju[9].

No nije Google jedini koji ulaže u Internet stvari i u umrežavanje doma u svrhu olakšavanja života i zaštite životnog prostora. Presence je besplatna aplikacija koja omogućuje korisniku da stari uređaj, mobilni telefon ili tablet, iskoristi na sličan način kao i Nest Cam Indoor, odnosno da ga pretvori u kameru koja provjerava da li postoji kretanje i ukoliko postoji da obavijesti korisnika i ponudi mu da pogleda što se događa. Ukoliko korisnik nije u mogućnosti odmah pogledati , video isječak se sprema i šalje na server gdje je dostupan korisniku. Međutim, mana koju Presence ima, odnosno koja ga čini slabijom verzijom od Nest Cam Indoora je ta da ne omogućuje rotaciju kamere niti prijenos zvuka.

Jedan od najboljih primjera kako će Internet stvari utjecati na život ljudi u bliskoj budućnosti su umreženi automobili. Automobilska industrija će se razvijati prateći tri glavna trenda u razvoju, a to su:

- Automatizam vožnje
- Električni sustavi i električni pogon
- Umreženost

Da razvoj industrije ide u tom smjeru može se zaključiti po činjenici da je takav razvoj već počeo jer već imamo dosta primjera. Jedan od njih je samo-vozeći automobil koji je razvio

Google X, poduzeće koje se bavi istraživanjem i razvojem. Uređaji potrebni da automobil bude samo-vozeći su uspješno instalirani u nekoliko različitih automobila, uključujući Toyotu Prius, hibridni automobil čiji pogon radi na tradicionalni motor sa unutarnjim izgaranjem te na električni pogon, Audi TT i Lexus RX450h. Sva tri trenda razvoja automobila su povezana te je razvoj automatiziranja vožnje uvjetovan elektronikom samog automobila i umreženosti samih sustava. A umrežavanje sustava te slanje podataka o vožnji na server i analiza tih podataka u stvarnom vremena je prvi korak prema budućnosti automobilske industrije. Prve stvari koje se umrežavaju su sustav informacija i zabave (eng. *infotainment*) i kontrolna ploča u automobilima, a umrežavanje istih će otvoriti put mnogim novim mogućnostima i poboljšanjima koje donosi Internet stvari. Neki primjeri poboljšanja koje umrežavanje pruža su eCall usluga, bCall usluga[14], usluge kontrole voznog parka kod službi za iznajmljivanje automobila te analiza podataka o vožnji za tvorca originalnih dijelova (eng. *Original Equipment Manufacturer,* kraće OEM) i za njihove dobavljače[1]. Uzimajući u obzir automobile koji idu na električni ili hibridni pogon, postoje sustavi koji će omogućiti kontrolu potrošnje goriva, rute do najbližih stanica za punjenje baterija te konstantno praćenje dijagnostike svih sustava.

Kontrolna ploča može poslužiti kao izravna konekcija između OEM-a i korisnika te je kao takva najvažniji element koji se umrežava. Ona omogućava korisniku da vidi sve potrebne podatke o stanju podsustava automobila kojime upravlja. Osim proizvođača, zainteresiranost za kreiranje su pokazali Apple i Google te se može figurativno reći da trenutno vode bitku tko će kreirati taj sustav. Ukoliko proizvođači odluče prepustiti kreiranje sustava na kontrolnoj ploči nekom od divova pametnih telefona, smanjiti će sebi troškove proizvodnje, međutim izgubit će veliki dio kontrole, kao i mogućnost izravne komunikacije sa korisnicima koja daje mogućnost razvijanja pozitivnih odnosa. Ako se odluče samo proizvoditi kontrolne ploče i sustav podrške, troškovi proizvodnje će biti veći, ali će zauzvrat imati mnogo veću kontrolu nad svojim proizvodima i već spomenutu komunikaciju. Međutim postoji i treća opcija, a to je nekakva sredina između prethodne dvije. Ta sredina bi bila aplikacija koja spaja pametni telefon sa već postojećim sustavom koji su proizvođači instalirali. Korisnik bi sam odabrao što želi da mu se prikaže na pametnom telefonu, a što na kontrolnoj ploči. Glavna prednost takve aplikacije je da omogućava pristup novim aplikacijama prema sučelju kontrolne ploče i što bi korisnik sam odabirao koje podsustave da mu se prikažu. Takvo rješenje bi najviše pogodovalo krajnjim korisnicima jer bi dobili najbolje od oba svijeta jer bi stručnjaci automobilske industrije morali usko surađivati sa najvećim stručnjacima Apple-a i Google-a da ostvare savršenu uslugu[15].

Veliku prednost umrežavanja automobila bi imala osiguravajuća društva jer bi imali uvid u način vožnje svakog pojedinca koristeći aplikaciju za kontrolu korištenja(eng. *Usage-base insurance*, kraće UBI) te bi svoje police mogli prilagoditi svakom pojedincu posebno.

UBI aplikacija bi imala pristup kilometraži, prosječnoj brzini, načinu kočenja vozača, GPS lokaciji, potrošnji goriva, da li često korisnik vozi po mraku i vikendima. Ti podaci bi se onda uspoređivali sa ostalima koje imaju u svojim sustavima, te bi temeljem tih rezultata stvarale personalizirane police osiguranja koje bi osiguravajućim kućama snižavale rizik, a dobrim vozačima bi police mogle biti po nekim procjenama do 30% manje. Postoje i druge posljedice uvođenja UBI aplikacije, odnosno sekundarne posljedice koje nisu direktno povezane sa uvođenjem i korištenjem. Jedna od najvećih sekundarnih posljedica bi bila povećanje 'mirnijih' vozača na ulicama. Postoje dva razloga za tu pretpostavku, jedan bi bio smanjenje polica osiguranja jer bi vozači vozili opreznije da izbjegnu veće cijene osiguranja. Drugi razlog je što bi i policijski službenici mogli dobiti uvid u prosječnu brzinu svakog vozača i GPS lokacije, odnosno rutu kojom je vozio. Vozači koji već imaju jeftinije police bi pazili da im se police ne povećaju. Ukoliko dođe do sudara svi podaci o trenucima prije sudara bi bili dostupni osiguravajućim kućama te bi isplate naknada bile niže ako vozač nije poduzeo sve potrebne mjere da izbjegne sudar ili ublaži štetu[15].

No nisu tehnološki divovi jedini koji razmišljaju o Internetu stvari i njegovom utjecaju na svijet. I političari se već neko vrijeme pripremaju za uvođenje Interneta Stvari i regulaciju istog. U Europskoj Uniji 1999. godine predstavljen je koncept eCall[14]. Dvije godine nakon toga eCall je predstavljen kao projekt no nekoliko je puta odgađan zbog problema sa tehnologijom i implementacijom. 2013. je napokon prihvaćen i dobio je rok od dvije godine da se ostvari. 28.4.2015. Europski Parlament je izglasao da svi novi automobili od travnja 2018. godine moraju imati ugrađen eCall, sustav koji bi po procjenama trebao skratiti vrijeme potrebno da hitna pomoć dođe na mjesto nesreće. Koncept eCalla je jednostavan, ukoliko podaci u automobilu prikazuju da bi moglo doći do nesreće ili ako se nesreća već dogodila, automatski se uspostavlja komunikacija između putnika unutar automobila i operatera hitnog broja, 112, bez obzira gdje se nesreća u Europskoj Uniji dogodila. Osim poziva, šalju se i GPS koordinate tako da hitna pomoć zna točnu lokaciju gdje se nesreća dogodila. Način na koji eCall zna da se dogodila nesreća ili da će se dogoditi je da nazove 112 u slučaju ekstremno naglog zatezanja sigurnosnih pojaseva, naglog kočenja, zvuka vrlo jakog udara te aktiviranju senzora na prednjim i stražnjim branicima. Drugi način poziva je pritisak na tipku koja će se nalaziti na kontrolnoj ploči. Dok god se ne dogodi nesreća eCall je u stanju mirovanja, odnosno aktivira se jedino na podražaje[14].

Pred Internetom stvari je mnogo izazova u budućnosti. Istraživanja koja se provode zadnjih nekoliko godina polako prerastaju u inovacije, nove tehnologije postaju dostupne, ali postoje neki problemi koji se još moraju razriješiti prije nego Internet stvari postane stvarnost. Postoje problemi koji su tehničke prirode, poput sigurnosti, pouzdanosti, kompleksne integracije i operabilnosti te standardizacija svih sustava, ali postoje i psihološki problemi, hoće li građani prihvatiti IoT. Problem mogu predstavljati i postojeći sustavi jer je većina

sustava zatvorenog tipa i vertikalne orijentacije, postoje razine prava koja omogućuju korisnicima pristup, dok Internet stvari teži sustavima otvorenog tipa i horizontalne orijentacije. Tehnologije koje omogućuju IoT mogu se podijeliti u 3 kategorije: tehnologije koje daju 'osjetila' stvarima, tehnologije koje procesuiraju informacije i tehnologije koje pružaju sigurnost i privatnost korisnika. Prve dvije kategorije su nužne za ostvarivanje Interneta stvari, dok je treća kategorija nužna za prihvaćanje IoT-a od strane potencijalnih korisnika. Mnoge postojeće tehnologije su se počele naglo unaprjeđivati u zadnjih nekoliko godina, poput[8]:

- Komunikacija
- Mrežna tehnologija
- Otkrivljivost mreže(eng. *discoverability*)
- Obrada podataka i signala
- Skladištenje energije
- Upravljanje mrežom
- Interoperabilnost, tehnologija koja spaja više različitih sustava u jedan

3. Sigurnost i privatnost Interneta stvari

Iz dosadašnjih primjera se lako može zaključiti da će Internet stvari donijeti mnogo novina u svaku poru društvenog života ljudi, od domova, osobnih automobila pa sve do poslovanja i organizacije gradova. Cijeli svijet koji nas okružuje polako, ali sigurno postaje automatiziran. Svaka stvar se povezuje sa Internetom te sama donosi odluke koje bi trebale biti najbolje za ljude. No postoje i problemi sa tom „utopijom“ kako se predviđa da će izgledati budućnost, a to je prije svega privatnost pojedinaca u okruženju Interneta stvari. „Mora postojati sloj sigurnosti koji ide iz računalnog čipa prema Internetu. Naravno, želite da informacije o vašem zdravlju idu do vašeg liječnika. Ali ljudi moraju osjećati sigurnost da ti podaci ne idu negdje drugdje“ kaže Michelle Dennedy iz McAfee poduzeća koje se bavi sigurnošću softvera[17]. Problem sa povezivanjem stvari u Internet stvari je zaštita RFID (radio frekvencijska identifikacija) čipova koji se koriste da bi se stvari spojile u IoT. Jeftinije i brže je napraviti čip koji će samo prikupljati i slati podatke, a jeftinije i brže bi moglo povećati zaradu organizacija i poduzeća koja nude takve usluge. Problem se nalazi i u činjenici da je tržište dosta veliko i da ima mnogo 'igrača' koji sudjeluju u Internetu stvari što znači da će biti mnogo nadmetanja. Naravno, veća poduzeća će posvetiti više pažnje sigurnosti i privatnosti svojih klijenata te će to prikladno i naplatiti. Uzmimo za primjer Alarm.com koji pruža klijentima mogućnost da instaliraju video nadzor u svojim domovima te da upravljaju sa kamerama preko Interneta. Osim video nadzora tu su i senzori koji otkrivaju kada se koji ulaz u kuću, bila to vrata ili prozor, otvore te u slučaju da se korisnik nalazi izvan kuće, odmah dobije obavijest o događaju koja sadrži detalje poput gdje je senzor očitan, u koliko sati i video snimak najbliže kamere. Dodana vrijednost koju pružaju je što se sve sprema na njihovim serverima te tako mogu pružiti veću sigurnost podataka, a tu veću sigurnost ostvaraju tako što njihovu uređaji mogu komunicirati jedino sa njihovim serverima čime eliminiraju mogućnost da netko drugi se spoji na spomenute uređaje i preuzme podatke[19].

3.1. Privatnost podataka

Da bi se moglo opisati kako se privatni podaci mogu narušiti i povrijediti u Internetu stvari, prvo moramo shvatiti što je točno privatnost. Međutim, ne postoji jasna definicija privatnosti, ali termin privatnosti se često koristio kroz povijest i bio je predmet mnogih debata. Kad se govori o privatnosti, najstarija je Aristotelova podjela na društvenu sferu politike, polis, i privatnu sferu obitelji, oikos, kao dvije potpuno različite sfere života svakog pojedinca.

Prema Westinu (1968.) privatnost pruža individualnim osobama i grupama u društvu očuvanje autonomije, oslobađanje od pretvaranja, vrijeme za samoprocjenu i zaštićenu komunikaciju. Nakon Drugog svjetskog rata napredak elektroničnih uređaja je počeo povećavati prijetnje očuvanja privatnosti u društvu. No prijetnja nisu bili uređaji nego i društvo koje je postalo otvorenije i koje se počelo mijenjati, a te promjene su želje društva da dobije više informacija o životima i navikama određenih javnih pojedinaca, a tehnologija je počela davati pristup javnosti tim informacijama[20].

DeCew u svojem radu „Privatnost“ (engl. *Privacy*) iz 2013. objašnjava različita viđenja privatnosti kroz povijest i u različitima kulturama. U tom radu DeCew pokazuje kako nekoliko različitih filozofa doživljava te kritizira koncept privatnosti. Za svu literaturu o privatnosti, DeCew kaže da se može podijeliti u dvije kategorije, redukcionizam i koherentizam. Glavna karakteristika redukcionista je da kritiziraju privatnost, dok koherentisti brane temeljne vrijednosti koje privatnost pruža. Kao jednu od najvećih kritičarki privatnosti spominje Judith Jarvis Thomson koja smatra da koncept privatnosti kao ljudskog prava ne bi trebao postojati jer sve što se smatra privatnošću se može pokriti sa drugim pravima, poput imovinskog prava. Ona smatra da je privatnost samo skup nekolicine drugih prava koje čovjek ima. Nadalje DeCew citira Richarda Posnera koji kritizira privatnost ne kao nepotrebno pravo, nego kao pravo nije ekonomsko. Za primjer uzima pisma preporuke i kaže kako takva pisma gube vrijednost ukoliko dođu u ruke onih na koje glase. Osim pisama preporuke spominje se i sakrivanje podataka ili selektivno objavljivanje podataka koje služi da prevari one kojima su podaci namijenjeni ili da ih izmanipulira. Još jedna u nizu kritika privatnosti je feministička kritika. Privatnost doma bi mogli iskoristiti zlostavljači da prikriju fizičko i psihičko zlostavljanje te iskorištavanje žena. Međutim tu dolazi do problema. Privatnost doma se može koristi kao štit protiv intervencije države, ali ako ne postoji privatnost sve je izloženo državi na upravljanje. Problem je naći pravi način očuvanja privatnosti, ali da ta privatnost ne sprječava državu da intervenira u slučaju nasilnog ponašanja. DeCew opisuje i vrijednosti privatnosti. Jedna od glavnih vrijednosti privatnosti je kontrola informacija, odnosno privatnost je sposobnost pojedinca da odabere kada će, kako, koji sve podaci i u kolikoj mjeri biti dostupni drugim pojedincima ili društvu. Glavni osobni podatci koje ljudi ne žele dijeliti javno, poput podataka o zdravlju, plaći, težini, seksualnoj orijentaciji su dokumentirani onda kada su dostupni javnosti, odnosno nakon što su objavljeni u novinama, sudskim spisima ili nekim drugim javnim dokumentima. Nakon što podaci postanu dokumentirani više ne može postojati invazija privatnosti ukoliko se ti podaci opet objave. Kao veliku vrijednost privatnosti spominje se očuvanje ljudskog dostojanstva. Ovdje DeCew citira Edwarda J. Blousteine (1964.), privatnost treba čuvati dostojanstvo pojedinca tako što ga čuva od snimanja, prisluškivanja, slikanja i sličnih stvari bez njegovog znanja[22]. Privatnost se povezuje sa intimnošću i društvenim vezama jer omogućava slobodu pojedincu da definira sam sebe i

svoje odnose s drugim ljudima. DeCew ovdje citira Frieda (1970.) koji opisuje privatnost kao ključni aspekt za odnose pojedinca sa drugim ljudima iz društva i ugrožena privatnost je prijetnja integritet pojedinca kao osobe[22].

Osim gore navedenih opisa privatnosti postoji i Internet privatnost. Internet privatnost je privatnost i sigurnost osobnih podataka koji se objavljuju preko Interneta. Taj izraz se koristi za tehnike i tehnologije koje se koriste da bi se sačuvali osobni i osjetljivi podaci tijekom komunikacije preko Interneta. No problem sa očuvanjem privatnosti i privatnih podataka na Internetu je u kreiranju jednostavnih rješenja i sustava koji bi se mogli iskoristiti u svakodnevnom životu, čija sigurnost nije na zadovoljavajućoj razini.

Na konferenciji za privatnost na Internetu stvari koju je organizirao TRUSTe 10. srpnja 2014. glavna rasprava se vodila oko ogromnog potencijala koji Internet stvari nudi i o mogućem žrtvovanju privatnosti u svrhu napretka. Jedan od govornika, Paul Rogers dao je primjer kako Internet stvari i golema količina podataka (eng. *Big Data*) mogu pomoći poslovanju izmišljene bolnice. Poboljšanje koje je naveo je u tome da se prate proizvodi koje liječnici koriste i njihova količina. Ukoliko jedan od liječnika koristi tri puta više gaze od prosjeka bolnice, nadležni bi bili obaviješteni o tome putem aplikacije i mogli bi porazgovarati s tim liječnikom oko njegove tehnike u svrhu poboljšanje iste i smanjenja korištenja gaze. Međutim taj primjer ima i negativnu stranu koju je idući govornik, Janna Anderson pokazala, a to je da taj izmišljeni liječnik koristi tri puta više gaze jer je to bolje za pacijente. Taj primjer pokazuje da će Internet stvari biti od velike koristi, ali samo ako bude upotrjebljen na pravi način, odnosno obradu podataka u začecima korištenja novog Interneta stvari bi trebao odrađivati čovjek[18].

3.2. Zakon o privatnosti u Europskoj Uniji

S razvojem Interneta stvari, poslovanje većine poduzeća će se ubrzati i olakšati, međutim to znači da će poduzeća brže skupljati podatke o klijentima i koristiti iste. Da bi se državljani Europske unije zaštitili, Europska Komisija je napravila veliku reformu zakona o zaštiti osobnih podataka. Nova regulativa i direktiva su objavljenje 4. svibnja 2016. godine u službenom glasilu Europske unije te su se počele primjenjivati u svibnju 2018. godine. Razlog čekanja dvije godine između izglasavanja i primjene je da bi se dalo vremena članicama da prilagode svoje zakone novoj direktivi. Razlika između direktive i regulative je ta da direktivu uvode i provode svaka zemlja posebno, a regulative postaju zakon unutar Europske unije i ne mogu se mijenjati. Ono što ova regulativa mijenja je to što je dosad odgovornost o osobnim podacima bila samo na vlasniku podataka, a nakon što se uvede regulativa, svatko tko ima pristup podacima, od poduzeća koje prikuplja podatke za poslovanje do trećih strana koje pružaju samo uslugu skladištenja istih postaju odgovorni ako

se štogod dogodi s tim podacima. Osim odgovornosti regulativa se odnosi i na razmjenu podataka o državljanima Europske unije izvan njenih granica, odnosno zahtijevati će se od poduzeća koje želi podatke proslijediti izvan granica da se temeljno pobrine za zaštitu istih inače neće biti dozvoljeno da se podaci proslijede. Vlasnici podataka će moći zatražiti od poduzeća koje je prikupilo njihove podatke da im dostave sve podatke koje imaju o njima, a zakonski rok koje će poduzeće imati za dostavu je 20 dana. Osim dostave podataka, regulativa će omogućiti vlasnicima da zatraže da se svi njihovi podaci obrišu iz njihovih baza. To bi moglo predstavljati probleme određenim sustavima i poduzeća će se morati pripremiti za takve zahtjeve prije nego regulativa dođe u opticaj. Period od dvije godine do stupanja na snagu nove regulative pruža poduzećima dovoljno vremena da se pripreme za nove zahtjeve i mogućnosti koje će morati osigurati klijentima. Ova regulativa je donijeta sada iz razloga što se Internet stvari sve više i više upotrebljava i razvija, a veliki problem koji mnogi vide s istim je upravo privatnost korisnika takvih sustava. Europska komisija se nada da će s ovom regulativom smanjiti sumnje građana u zaštitu privatnosti[16].

3.3. Privatnost u Internetu stvari

Privatnost na Internetu je pojam koji je različit za svakog pojedinca slično kao i u stvarnom svijetu. Koje podatke će pristati podijeliti i u kojoj količini ovisi o povjerenju stranici na kojoj se nalazi na Internetu. Isto tako svatko dijeli vlastite informacije s drugim ljudima s obzirom koliko im vjeruje da će ta osoba čuvati iste. Ljudi žele sigurnost da će njihove informacije biti korištene samo od strane sustava kojima vjeruju. Većina sustava na Internetu razmjenjuje vlastite usluge u zamjenu za informacije o korisnicima, te onda te informacije koriste za prodaju oglasnog prostora. Ebay prikuplja podatke o tome što korisnik pretražuje te prilikom svakog slijedećeg spajanja predlaže istom korisniku slične artikle. No povjerenje ljudi prema Internetu raste, a u prilog tome ide činjenica da su se razvili sustavi poput Ubera i Airbnb-a kojima se strancima omogućava ulazak u osobni automobil korisnika i njegov dom[17]. Internet stvari prikuplja golemu količinu podataka o korisniku, te postoji problem da bi se te informacije mogle koristiti u svrhe koje nisu pogodne korisniku. Problem koji je poseban za Internet stvari i privatnost je da u tom sustavu postoji mnogo uređaja koji prikupljaju i razmjenjuju podatke korisnika. Da bi korisnik mogao vjerovati cijelom sustavu, mora vjerovati svakom od uređaja, senzora i kamera da podatke neće poslati na krivu lokaciju i da je te podatke nemoguće otuđiti. Spojeni uređaji u Internet stvari prikupljaju i procesuiraju toliko podataka da je zaštita svih njih veoma teška. Pametni telefoni koje gotovo svi u današnje vrijeme koriste, osim što pružaju mnogo usluga korisniku, ujedno i stvaraju golemu količinu podataka o istom korisniku. Sve što korisnik radi na telefonu se sprema, a isto rade i ostale pametne stvari koje sve više ulaze u domove, od pametnih televizora,

frižidera do ulaznih senzora i rasvjete. S obzirom na golemu količinu podataka koja se prikuplja, mijenja se i odnos ljudi prema privatnosti. Pametne stvari olakšavaju život korisnicima, te zbog toga korisnici žrtvuju dio svoje privatnosti[23].

3.4. Sigurnost na Internetu

Sigurnost se može definirati na mnogo načina. Prva stvar na koju ljudi pomisle kad se spominje sigurnost je zaštita od opasnosti te bi se i tako mogla opisati sigurnost na Internetu. Razlika je što su opasnosti koje vrebaju na Internetu usmjerene na informacije koje pojedinci dijele. Stoga bi se sigurnost na Internetu mogla opisati kao obrana digitalnih informacija od slučajnih i zlonamjernih prijetnji. Ta obrana uključuje otkrivanje opasnosti, prevenciju i odgovor na napad. Sigurnost koju poduzeća i organizacije ostvaruju na Internetu se dijeli na dva koraka. Prvi korak je fizička sigurnost, odnosno sigurnost ljudi, uređaja i mreže od fizičkih napada. Postoji nekoliko opasnosti koje fizička sigurnost mora otkloniti, između ostaloga to su prirodne katastrofe, požari, krađa i uništavanje. Zgrade i prostorije u kojima se nalaze ljudi, uređaji i mreže moraju biti dostupni samo zaposlenicima. Ukoliko bi napadač dobio pristup mreži mogao bi ukrasti podatke, obrisati ih ili ubaciti štetni program direktno u sustav poduzeća ili organizacije. Drugi korak je sigurnost podataka. Napadač može pristupiti mreži i podacima i sa udaljenje lokacije ukoliko oni nisu dovoljno dobro zaštićeni. Sigurnost podataka se dijeli na nekoliko kategorija, glavna je sigurnost aplikacija. Aplikacije koje poduzeća ili organizacije koriste moraju se moći obraniti od pokušaja nelegitimnog pristupa, krađe, uređivanja ili brisanja podataka. Na nekoliko načina se ostvaruje sigurnost, a neki su aplikacijski vatrozid, programi enkripcije podataka i biometrijska autentikacija. Druga kategorija je zaštita 'oblaka' (eng. *Cloud security*). 'Oblak' je način računalne infrastrukture i aplikativni model koji služi za brzi pristup podacima, mreži i uslugama sa minimalnim upravljačkim naporom. Glavni problemi zaštite Oblaka su identificiranje, dozvola pristupa i privatnost podataka koji se nalaze u Oblaku. Nadalje, zaštita pristupnog uređaja, to je uređaj koji se koristi za pristup mreži, a to može biti stolno računalo, prijenosno računalo, pametni telefon, tablet ili računalni terminal. Takvi uređaji moraju prvo biti autorizirani da bi mogli dobiti pristup mreži. Iduća kategorija je sigurnost aplikacija koje se koriste za pristup mreži. Te aplikacije moraju onemogućiti pristup napadačima, a to se ostvaruje pomoću enkripcije. Mobilna sigurnost je sigurnost prijenosnih uređaja koji imaju pristup mreži. Takvi uređaji moraju imati zaštićen pristup dok su spojeni na mrežu da se spriječi curenje podataka ukoliko je neki drugi uređaj spojen na njih preko bežične mreže. Sama sigurnost na Internetu se ostvaruje služeći se jednom od strategija kojom se sigurnost ostvaruje, a neke strategije su[24]:

- dubinska obrana – strategija koja koristi slojevitu zaštitu od napada,
- strategija najmanjeg prava pristupa – ograničava broj korisnika i korisnički pristup na najnižu moguću razinu u svrhu povećanja sigurnosti,
- kontrola ranjivosti – pristup gdje se provjeravaju slabosti, identificiraju se te se otklanjaju,
- kontrola rizika – pristup gdje se identificira, procjenjuje i kontroliraju rizici mrežnog sustava,
- kontrola koda – pristup gdje se provjerava postojeći kod, nadopunjuje se sa novim mogućnostima koje se prvo testiraju i instaliranjem zakrpa koje pokrivaju 'rupe' u aplikaciji.

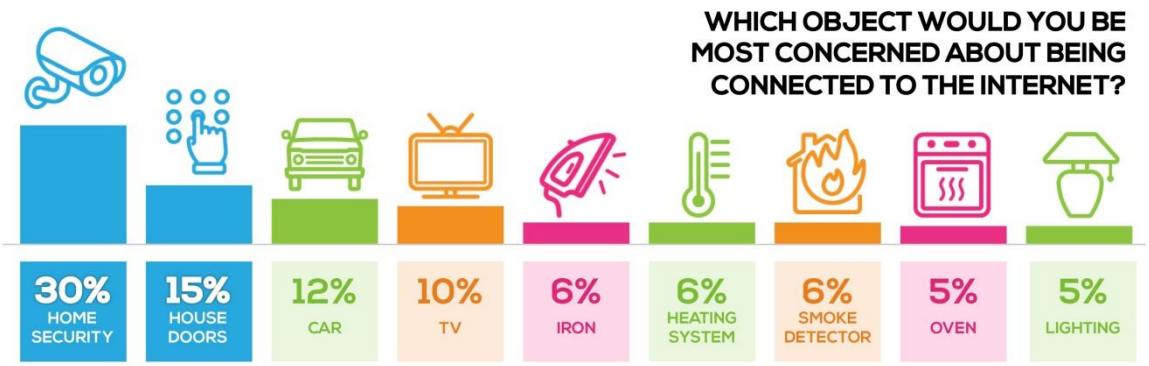
3.5. Sigurnost Interneta stvari

Glavni problem Interneta stvari su upravo prethodne dvije točke, privatnost korisnika i sigurnost podataka koja se nalazi unutar Interneta stvari. Na slici 7 vidimo istraživanje mišljenja javnosti pod nazivom 'Utjecaj povjerenja na IoT' (eng. *The Impact of Trust on IoT*) koji je proveo MEF 2016. godine u suradnji sa AVG-om. Tehnologija koja nam je već danas dostupna može omogućiti ostvarivanje Interneta stvari u mnogim sferama života, ali kao što se vidi iz ovog istraživanja, glavna prepreka je povjerenje javnosti u sigurnost povezanih uređaja i stvari. Istraživanje je obuhvatilo preko 5000 ljudi u 8 različitih država na 5 kontinenata i pokazalo da 60% ljudi je zabrinuto oko povezivanja svakodnevnih stvari međusobno i u Internet.

Slika 7: Povjerenje prema Internetu stvari (izvor: MEF anketa)

Ono što najviše zabrinjava ljude je njihova privatnost za koju čak 62% ispitanika smatra da će biti narušena, a 54% smatra da podaci koje uređaji budu dijelili neće biti sigurni. Zanimljivo je da svaki peti ispitanik strahuje da će računala preuzeti kontrolu nad svijetom, a svaki 10 smatra da IoT neće donijeti osjetna poboljšanja ni u jednu sferu života[25].

Kad se priča o Internetu stvari, prva velika prednost koju pruža je olakšavanje svakodnevnog života, a to se omogućava ostvarivanjem pametne kuće. Međutim na slici 8 vidimo da preko 80% zabrinutosti ljudi oko spajanja stvari u Internet se odnosi na stvari koje bi se nalazile u pametnoj kući sa čak 30% ljudi koji su zabrinuto oko sigurnosti vlastitog doma. 15% ljudi se izjasnilo da ih najviše brine zaključavanje vrata u pametnim kućama i da smatraju da bi IoT vrata mogla omogućiti uljezima i lopovima da im ulaze u kuću bez njihovog znanja.



Slika 8: Zabrinutost javnosti oko spajanja stvari na Internet (izvor: MEF anketa)

Velika stavka koja je bitna ljudima oko Interneta stvari je transparentnost. 41% ispitanika se izjasnilo da je transparentnost ekstremno važna i 11% koji su rekli da je veoma važna. Todd Simpson, direktor u AVG-u je izjavio: „MEF-ovo istraživanje pokazuje konstantno opadanje povjerenja klijenata, koje nastavlja silaznom putanjom kako se rat sa privatnošću prolongira, ostavljajući klijente da odluče koji podaci su vrijedni razmjene“[26].

S obzirom da su privatnost i sigurnost najveći problemi implementaciji i primjeni Interneta stvari, postavlja se pitanje što sve poduzeća koja planiraju provesti implementaciju istih primjenjuju da se zadovolje krajnji korisnici. Jedna od opcija povećanja sigurnosti je minimalizacija podataka. To je koncept u kojem poduzeća koja nude uslugu uzimaju najmanju količinu podataka od klijenata koja je potrebna za funkcioniranje usluge. Na primjer, ukoliko točna lokacija uređaja nije neophodna za njegovo funkcioniranje onda nema

potrebe da se ta informacija prikuplja i sprema u bazu podataka. Ukoliko postoji opcija da će u budućnosti informacija biti potrebna za neku novu opciju, dovoljno je spremiti neku sličnu informaciju, na primjer poštanski broj ili ime grada u kojem se nalazi. Uređaji u Internetu stvari ne bi trebali prikupljati sve moguće podatke samo zbog šanse da će ti podaci biti korisni u budućnosti jer to može stvoriti nepovjerenje korisnika. Minimalizacija kao opcija služi za eliminiranje dvije moguće prijetnje. Prva je činjenica da ogromna baza podataka povećava napade na istu, odnosno što je više podataka u bazi veća je šansa da će netko htjeli otuđiti te iste podatke. Drugo, podaci koji se čuvaju duže nego je to potrebno povećavaju rizik da će ti podaci biti iskorišteni za nešto što korisnik nije pristao da se koriste. Minimalizacija podataka nije jedino dobra za klijente, dobra je i za poduzeća jer manje podataka koji su spremljeni smanjuje troškove poduzeća te se povećava povjerenje klijenata prema poduzeću koji uzimaju i koriste samo one podatke koji su neophodni za pružanje usluge. Drugi način povećavanja sigurnosti je pružanje kontrole klijentu. To se odnosi ne samo na korištenje uređaja Interneta stvari već i na odlučivanje koje će sve podatke taj uređaj prikupljati. Nitko ne želi da ima uređaj u vlastitome domu koji će prikupljati podatke za koje korisnik nije svjestan da prikuplja. Poduzeća bi morala klijenta obavijestiti koje sve podatke uređaj može prikupljati i u kojoj mjeri te tražiti od klijenta odobrenje da omogući uređaju prikupljanje samo onih podataka na koje klijent pristaje. Pristup poduzeća koji tretira sve klijente jednako i od svih traži jednaka dopuštenja oko prikupljanja nije nikako dobar jer tako mogu samo povećati ionako veliko nepovjerenje ljudi prema Internetu stvari[27].

Još jedan problem sigurnosti Interneta stvari na koji Gorodyansky ukazuje je činjenica da 90% podataka na Internetu stvoreno u posljednje dvije godine (članak je iz 2015.), a Internet stvari će omogućiti vrlo brzo spremanje velike količine podataka. Samo zbog toga sigurnost uređaja bi morala biti na prvom mjestu kad se govori o uređajima koji će se koristiti za Internet stvari[22].

4. Narušavanje privatnosti u IoT primjerima

Svi se slažu da je Internet stvari budućnost i da nosi mnoge prednosti, ali u prethodnom poglavlju smo vidjeli da postoji veliki problem sa povjerenjem budućih korisnika Interneta stvari, a najveći razlog za brigu se navodi privatnost podataka. No da li stvarno postoji razlog za toliko nepovjerenje? Nekoliko primjera Interneta stvari je već opisano kako funkcioniraju i kako bi se trebali implementirati, no nije spomenuto koje podatke zahtijevaju od korisnika ni kako će ti podaci biti iskorišteni. U nastavku ću koristiti već opisane primjere Interneta stvari te moguće načine na koji se narušava privatnost pojedinaca koji se koriste tim sustavima.

4.1. Narušavanje privatnosti u pametnoj kući

Prvi primjer je pametna kuća. Potrebni podaci za funkcioniranje bi, između ostaloga, bili lokacija kuće, broj ukućana, godine i spol ukućana, zdravstveni problemi itd. Postoji mnogo različitih opisa kako bi pametna kuća trebala izgledati i što bi sve trebala sadržavati, za ovaj primjer koristit je već napravljeno testiranje u kojem se koristila 'jednostavna' pametna kuća koja sama namješta termostat, kontrolira osvjetljenje, požarni alarm, ima pametnu kuhinju, video nadzor te su u IoT uključeni senzori na vratima i prozorima. Sigurnost trenutno postojećih pametnih kuća je testirana 2015. godine, a testiranje je provelo Synack, poduzeće specijalizirano za sigurnost. Testirali su 16 uređaja za automatizaciju domova, od kamera preko daljinskih upravljača do termostata. Način na koji su testirali uređaje je da su smislili nekoliko potencijalnih scenarija koje bi hakeri mogli koristiti da dobiju uvid u život korisnika. Prva simulacija je bila takozvana 'otvorena kuća', haker je imao pristup uređajima na dvije minute. Većina uređaja je uspješno položila ovaj test, odnosno fizički pristup uređajima nije pomogao hakerima da dobiju kontrolu. Drugi scenarij je bio ukradeni mobitel, u smislu da haker uspije pristupiti mobitelu korisnika na pet do deset minuta. Ovaj scenarij je pokazao velike mane trenutnog stanja uređaja koji su povezani u Internet stvari jer većina lozinki koje mobilna aplikacija koristi da dobije pristup uređajima u pametnoj kući, kao na primjer kamerama, su spremljene u tekstualnom obliku bez ikakve enkripcije ili su cijelo vrijeme spojeni bez potrebe za ponovnom autentikacijom što omogućuje napadaču pristup svim uređajima s kojima aplikacija komunicira. Idući scenarij je bio 'Internet kafić', odnosno što se događa ako je napadač na otvorenoj WiFi mreži koju koristi i korisnik, na primjer da provjeri kamere u pametnoj kući ili da provjeri jesu li vrata i prozori zatvoreni i zaključani. Smisao ove provjere je da se vidi da li napadač može presresti komunikaciju i preuzeti ili kopirati kontrolu da dobije pristup uređajima. Ponovno je bio isti problem kao i kod spremanja lozinki, odnosno komunikacija između mobilne aplikacije i uređaja pametne kuće je bila otvorena da ju napadač pročita i spremljena u tekstualnom obliku. To omogućuje napadaču da kopira tu istu komunikaciju i dobije kontrolu nad uređajima. Zadnji scenarij je bio modifikacija uređaja, odnosno da li napadač može instalirati svoj softver u sam uređaj da dobije kontrolu bez da uređaj ili proizvođač primijeti. U čak 93% slučajeva napadačima je trebalo svega 20 minuta da uspiju instalirati svoj softver, a nakon par pokušaja uspijevali su to učiniti ispod 5 minuta. No to nije problem samo sa IoT uređajima već sa velikom većinom uređaja te to pokazuje da proizvođači moraju mnogo pažnje posvetiti da se pristup uređajima ne dozvoljava nepouzdanima osobama. Ovo testiranje je pokazalo da nepovjerenje korisnika prema Internetu stvari ima podlogu, odnosno da trenutno postojeći IoT uređaji ne implementiraju dovoljnu zaštitu da bi sačuvali privatnost korisnika niti njegovu sigurnost. Čak i da napadač ne dobije kontrolu nad uređajima nego

samo uspije presresti podatke koje uređaji šalju stvara ogromni problem jer se time drastično narušava privatnost korisnika. Napadač može skupiti gomilu informacija od korisniku, može naučiti njegovu rutinu i ponašanje te dobiti pristup svim uređajima u njegovom domu[30]. Trenutno postoji mnogo izazova koje proizvođači i svi vezani za Internet stvari moraju riješiti, neki osnovni su[8]:

- Tržište ne investira dovoljno da bi se postigla zadovoljavajuća razina sigurnosti
- Definicija privatnosti nije ista u svim zemljama
- Trenutna rješenja zaštite su zamišljena da štite podatke unutar uređaja ili aplikacije, ali se ne mogu dijeliti s drugim uređajima niti pokrivaju komunikaciju između tih uređaja
- Potreba za zaštitom podataka je u suprotnosti sa ponašanjem proizvođača koji žele pristup ogromnoj količini podataka (eng. *Big Data*)
- Korištenje podataka prikupljenih za jednu aplikaciju u drugoj aplikaciji je suprotno od privatnosti

4.2. Narušavanje privatnosti u pametnom gradu

Drugi primjer Interneta stvari je bio pametni grad, odnosno grad koji je umrežen. Kao što je već opisano u primjeru veliki problem koji bi se riješio je problem parkiranja, odnosno svaki korisnik koji je spojen na mrežu grada bi mogao preko mobilne aplikacije dobiti informaciju gdje se nalazi najbliži parking na kojem ima mjesta. Osim parkiranja dobivao bi i upozorenja koje ulice da izbjegava zbog gužvi u prometu. Postoji još mnogo poboljšanja koja bi se mogla ostvariti u pametnome gradu, no idemo vidjeti kako se u pametnome gradu može narušiti privatnost pojedinca, odnosno stanovnika grada. Prvo što se nameće kao problem privatnosti je GPS lokacija svakog uređaja, odnosno mobitela kojeg korisnik koristi da bi se spojio na mrežu. Dok god je aplikacija uključena, netko u gradskoj upravi može točno locirati gdje se nalazi osoba, ili njen mobitel. Iako lociranje u svakom trenutku može biti od koristi, isto tako se može iskoristiti i protiv korisnika. U prethodnom poglavlju smo vidjeli da postoji problem sa količinom podataka koja je potrebna da uređaj koji je spojen u Internet stvari može raditi, pa tako i mobilna aplikacija kojom bi korisnik dobio pristup pametnom gradu bi zahtijevala određene osobne podatke, poput imena i prezime. Ukoliko bi napadač uspio dobiti pristup kontroli pametnog grada ili samo uvid u podatke, mogao bi vrlo lako otkriti za svaku rutinu za svakog korisnika, put kojim ide od posla do doma, gdje parkira, gdje jede, s kim se druži. No ne bi problem bio samo potencijalni napadač, nego bilo tko tko je zadužen

da nadgleda i kontrolira pametni grad. Pametni grad bi tako postao jedan veliki 'Big Data' kolektor. Sve što se događa u gradu bi se spremalo, svaka kretnja svakog pojedinca, a to bi moglo uzrokovati velike probleme sa privatnošću jer bi iz svih tih podataka se mogli napraviti profili svakog stanovnika grada. Na primjer, ukoliko nekoliko osoba su često skupa na istim mjestima i zajedno se kreću od mjesta do mjesta, te kretnje se mogu iskoristiti kao temelj da su te osobe u političkoj, socijalnoj ili religioznoj grupi. Slično tome, ti podaci mogu pokazati da pojedinac posjećuju homoseksualne barove, što bi se moglo protumačiti da je on ili ona homoseksualac, a taj podatak se smatra osjetljivom privatnom informacijom. Još jedan problem koji to može prouzročiti je ukoliko se 'Big Data' iskoristi za stvaranje profila osobe, te se na temelju tog profila toj osobi pošalje na kućnu adresu reklame koje se inače šalju homoseksualnim osobama, to bi moglo prouzročiti štetu osobi, pogotovo ukoliko je profil pogrešan. No poduzeće ili organizacija koja iskoristi taj profil osobe i pošalje takve promotivne reklame prema postojećim zakonima ne mora zatražiti pristanak korisnika da želi primati takve materijale[28].

4.3. Narušavanje privatnosti u transportu

Idući primjer Interneta stvari je bio umrežavanje transporta. Narušavanje privatnosti pojedinca u Internetu stvari transporta dosta je slično narušavanju privatnosti u pametnom gradu. Poslodavac zna u svakom trenutku gdje se vozač nalazi sa kamionom, zna brzinu kojom vozi, u kakvom stanju je roba, da li mora proći kroz gužvu i da li je možda prolaz zabranjen za kamione te kategorije. Naravno u kategoriju transporta ulaze i autobusi, a sa prijevozom putnika dolazi do još većeg problema sa zaštitom privatnosti. Osim položaja kamiona ili autobusa, poduzeće može pratiti i svaki pokret vozača. Konstantno praćenje težine, brzine i ispušnih plinova kamiona ili autobusa će snimiti radni vijek vozača vozila. Osim spremanja i praćenja svih tih podataka, Internet stvari će omogućiti i automatsko upozorenje službama za pomoć na cesti ukoliko se otkriju sigurnosni problemi poput potrošenih guma, problema sa kočnicama i sličnih problema. Osim tih problema, poduzeće može omogućiti i automatsko javljanje policijskim dužnosnicima ukoliko se primijete fizički ili psihički problemi vozača tijekom vožnje. Ta komunikacija o sposobnosti vozača i njegovom umaranju tijekom vožnje prema kontrolnom sustavu u poduzeću predstavlja probleme privatnosti. Jedan od problema kako se narušava privatnosti je i način na koji će sustav transporta Interneta stvari funkcionirati. Da bi mogao navoditi vozača do destinacije, komunikacija između uređaja u vozilu prema sustavu mora biti konstantna i dvosmjerna. Od vozila bi išli podaci o vrsti vozila, brzini, odredištu i podaci sa kontrolne ploče dok u drugom smjeru bi išli podaci o protoku vozila, zastojima, vremenu i podaci koje sam vozač bude zatražio da mu se dostavljaju. Svi ti podaci bi se u Internetu stvari spremali u bazu podataka

da ostanu kao predlošci za buduće vožnje na istoj ili sličnim relacijama. Sve te informacije mogu biti veoma korisne trećim stranama koje žele pratiti vozače, a to bi mogli biti policijski službenici, privatni detektivi, marketinške kompanije ili uhode. Osim što bi pratili put i javljali kakvo je stanje vozačima, ti sustavi bi mogli se koristiti da se planira putovanje unaprijed. Moguće bi bilo i napraviti profile putnika. Gradski autobusi koriste kartice koje su praktičnije nego kupovanje karata, ali zauzvrat omogućuju poduzećima da prikupljaju informacije o kretnjama korisnika, pa tako mogu pratiti koliko vremena ljudi provode na određenim lokacijama, kao na primjer supermarketima. Te podatke bi mogli iskoristiti marketinške kompanije za pravljenje profila slično kao u primjeru sa pametnim gradom. Podaci skupljeni tako pružaju još jednu prednost marketinškim poduzećima, a to je da mogu pratiti godine, visinu, težinu i spol ljudi koji idu na ista mjesta, vremena kada najčešće idu i koji put koriste te sve te podatke spojiti sa drugim podacima o građanima, usporediti ih i dobiti vrlo dobru prognozu prodaje određenih proizvoda. Problem je što pojedinci, odnosno korisnici transporta ne znaju da se svi ti podaci uzimaju i uspoređuju bez njihovog znanja i pristanka i to predstavlja veliki problem privatnosti[28].

4.4. Narušavanje privatnosti u zdravstvu

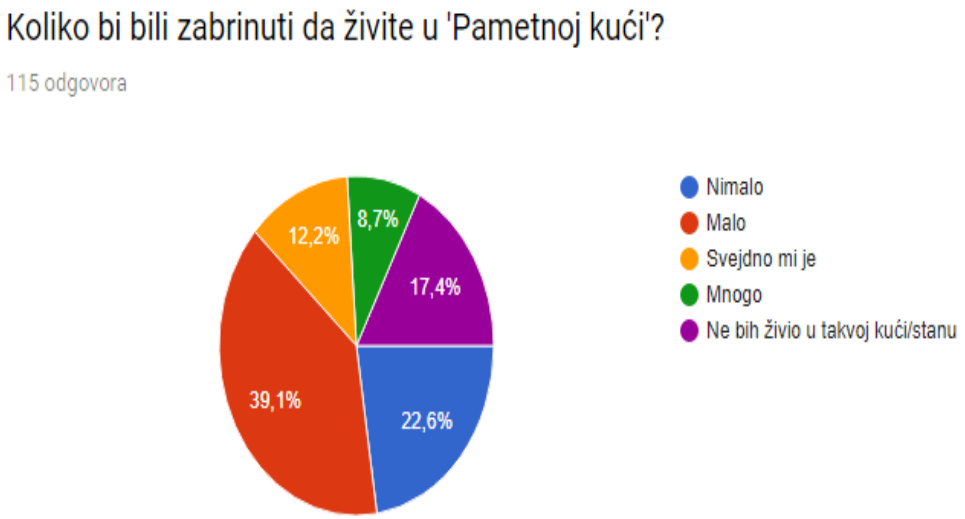
Posljednji primjer je umrežavanje zdravstva u Internet stvari. Princip bi bio da svaka osoba u zemlji ima pristup liječniku u bilo koje doba dana ili noći, odnosno najbliži liječnik bi trebao biti automatski obaviješten čim je pacijentu potrebna pomoć. Postoji nekoliko načina na koje se to može ostvariti, u ovom radu je već spomenut sat koji automatski mjeri tlak i u slučaju da dođe do probleme šalje obavijest na mobilni uređaj. Taj bi se sat mogao se povezati na umreženi sustav zdravstva i uputiti obavijest osobnom liječniku svaki dan o tlaku pacijenta koji ima zdravstveni problem i treba dnevno provjeravati. Problem koji se tu nadzire je sigurnost prijenosa tih informacija. Da bi liječnik znao čiji su podaci potrebno je poslati i identifikaciju osobe čiji podaci se šalju te bi tu moglo doći do krađe podataka ukoliko sat koristi otvorenu mrežu čime bi potencijalno pružio šansu napadaču da presretne komunikaciju i dobije pristup liječničkim zapisima.

5. Anketa

Internet stvari se već razvija dugi niz godina,ali još uvijek nije posve ukomponiran u svakodnevni život ljudi. Veliki gradovi razvijaju sustave kojima pokušavaju olakšati svakodnevnicu svojim građanima i gradskim planerima. Sve je više pametnih uređaja na tržištu, sve više ljudi se odlučuju na unaprjeđenje vlastitog doma u pametnu kuću, odnosno sve više uređaja koje kupuju su pametni uređaji. S obzirom na taj trend odlučio sam provesti anketu da bih dobio uvid koliko su ljudi upoznati sa Internetom stvari, koliko vjeruju takvim sustavima i kakva su njihova razmišljanja. Ispitanici su podijeljeni po spolu, godinama i završenom stupnju obrazovanja. Po godinama su podijeljeni s ciljem dobivanja uvida kako različite grupe funkcioniraju. Prva grupa su maloljetnici, druga je od 18 godina do 25, ovdje bi spadali studenti, treća grupa su mladi ljudi od 26 godina do 35 godina. Iduća grupa su stariji ljudi koji imaju dosta radnog iskustva ili su pred mirovinom, odnosno od 36 godina do 60, a zadnja skupina su bili umirovljenici i ljudi pred mirovinom. Bilo je 115 ispitanika, o toga 71 muškaraca i 44 žena. Najviše ispitanika su bili mladi ljudi koji su tek završili srednju školu ili su na fakultetu koji imaju između 18 i 25 godina, njih je bilo 65, drugi su od 26 do 35 godina, njih 29. Najviše ispitanika ima samo srednju školu završenu, 43% njih, nakon njih je 27,5% ispitanika koji su završili preddiplomski studij. Prvo pitanje je bilo jesu li upoznati sa pojmom Internet stvari, na što je 85% ispitanika odgovorilo potvrdno. Iduće pitanje je bilo da li bi htjeli živjeti u pametnoj kući, ovdje je 67,3% ispitanika reklo da bi to voljelo. Zanimljivo je da 75% muškaraca reklo da bi htjeli živjet u pametnoj kući dok je samo 55% žena to isto navelo. Što se tiče stupnja obrazovanja, čak 80% diplomiranih ispitanika je odgovorilo potvrdno naspram 60% ispitanika koji su završili srednju školu.

Graf 1

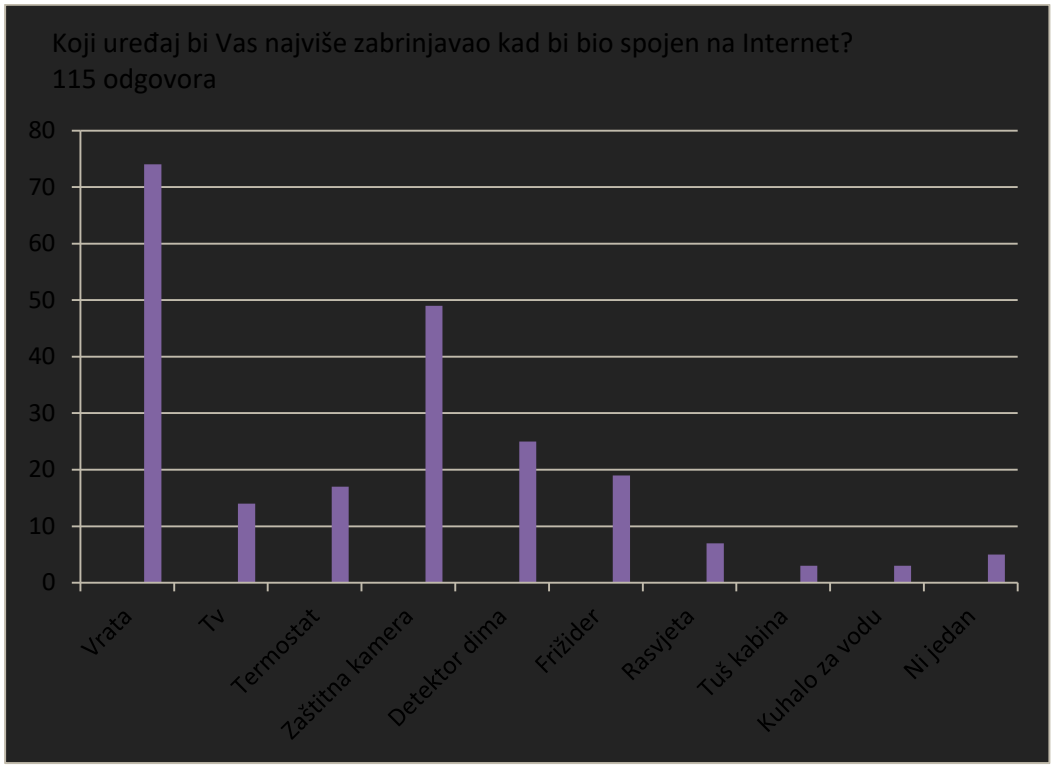
Kao što se vidi na grafu 1, tri četvrtine ispitanika smatra da bi se kontrola nad jednostavnim akcijama mogla prepustiti uređajima i pametnim stvarima. Iz ovog se može zaključiti da većina ispitanika smatra da se ne treba brinuti, odnosno da se može vjerovati proizvođačima koji se bave Internetom stvari, a to je većina i potvrdila u idućem pitanju gdje se tražilo od njih da objasne zašto smatraju da bi se moglo prepustiti kontrola. „Jednostavnije upravljanje i dovoljna razina sigurnosti“, „Jednostavniji život, može se kontrolirati na daljinu“ i „Trenutno živim u stanu gdje se automatski održava temperatura kao što se gasi struja i rasvjeta kada nikoga nema u stanu i to smanjuje iznose računa uz to sigurnije je ukoliko se nešto zaboravi ugasiti“ samo su neki od odgovora zašto smatraju da nije problem prepustiti kontrolu 'stvarima'. Međutim, ispitanici koji smatraju da ne treba prepustiti kontrolu dali su slijedeća objašnjenja: „Radi sigurnosti“, „Uređaji nisu usavršeni dovoljno da bi radili bez negativnih posljedica za ljude“ te „Jer volim biti u kontroli“. Ostali odgovori su uglavnom slični, dok se jedni boje zbog mogućih propusta u sigurnosti takvih sustava, drugi jednostavno ne žele prepustiti kontrolu.



Graf 2

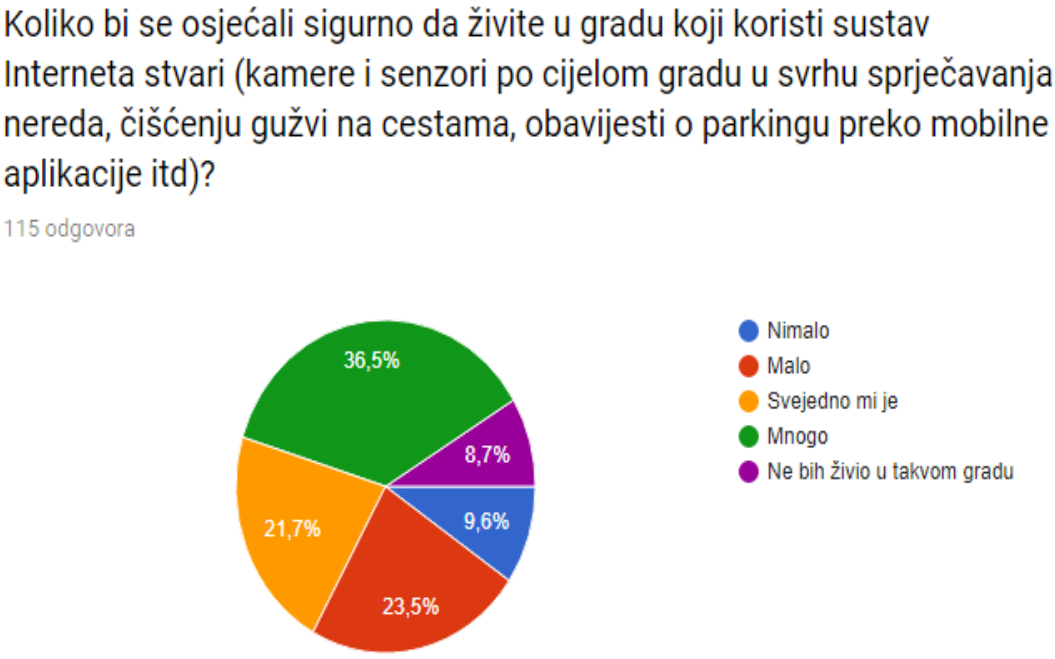
Na drugom grafu vidimo podjelu odgovora o zabrinutosti oko života u pametnoj kući. Postotak odgovora je sličan kao na pitanje koliko smatraju da se može kontrola prepustiti uređajima. 26% njih bi bilo mnogo zabrinuto ili ne bi uopće pristali živjeti u istoj, a 23,5% smatra da ne treba prepustiti kontrolu. Ovdje su postotci slični ukoliko se uzme u obzir stupanj obrazovanja, 25% ispitanika sa završenom srednjom školom su se izrazili da ne bi nimalo bili zabrinuti kad bi živjeli u takvoj kući, 20% ispitanika sa završenim preddiplomskim studijem, te 27% ispitanika koji su diplomirali. 48 muških ispitanika, ili 66% su se izjasnili da malo ili nimalo ne bi bili zabrinuti. Taj postotak je manji kod ženske populacije, 52% ih je

izjavilo malo ili nimalo. Na pitanje da objasne svoje razmišljanje, mnogi su kao glavni problem naveli sigurnost sustava. „Određena briga postoji jer su svi ti uređaji većinom povezani wifi-om te smo tako lakše podložni hakerskim napadima“, „Nije svejedno da ti netko može probiti zaštitu i kontrolirati tvoj dom, da netko skuplja informacije o tebi, a da to ni ne znaš“, „Ispočetka sigurno mnogo, ali ne zbog straha od tehnologije, već zbog hakera i straha od toga da me netko može cijelo vrijeme špijunirati“ su samo neki od odgovora iz kojih se da zaključiti da većina smatra kako sigurnost takvih sustava još uvijek nije na zadovoljavajućoj razini. No ima i onih koji smatraju da to nije slučaj. „Pametne kuće su budućnost“, „Zato što smatram da je to potpuno bezopasno“, „Dovoljno vjerujem tehnologiji“ su neki odgovori ispitanika koji se nimalo ili malo brinu o životu u pametnoj kući.



Graf 3

Na grafu 3 imamo rezultate s obzirom koji uređaj bi ispitanici naveli kao najveći potencijalni problem. Tu ponovno vidimo da je najveća briga usmjerena na zaštitu ulaza, odnosno vrata, a na drugom mjestu je zabrinutost da bi napadač mogao preoteti kontrolu nad kamerom te dobiti uvid u privatnost korisnika.



Graf 4

Jedan od sustava Interneta stvari koji se već uvodi u velikim i razvijenim gradovima u svijetu je sustav kontrole i nadgledanja grada. 45% ispitanika smatra da ne bi bilo sigurno živjeti u takvom gradu, odnosno smatraju da bi im privatnost bila narušena. No čak 34% ne bi imalo previše problema sa životom u takvom gradu. Zadnje pitanje je bilo 'Mislite li da ima razloga za brigu zbog razvoja Interneta stvari i prepuštanju kontrole uređajima i stvarima?' te je 69% ispitanika se izjasnilo da smatra da postoji opravdani razlog za brigu. I oko ovog pitanja postoji vidljiva razlika u razmišljanju muškaraca i žena. Svaki drugi muški ispitanik smatra kako ne postoji razloga za brigu, dok 1 od 4 ženskih ispitanica smatraju da ne postoji razloga za brigu. Zanimljivo je i da mlađi smatraju da ima razloga za brigu, dok su stariji suprotnog mišljenja. 64,5% ispitanika između 18 i 25 godina smatra da postoji opravdan razlog za brigu, iduća grupa, od 26 do 35 godina života, njih 55% smatra da ima razloga za brigu, dok u trećoj grupi, od 36 do 60 godina života, svaki drugi ima isto mišljenje. Razina obrazovanja ovdje ne igra ulogu, 57,7% ispitanika sa srednjoškolskim obrazovanjem smatra da ima razloga za brigu, taj postotak kod ispitanika sa preddiplomskim studijem je 60%, a sa diplomskim studijem je 54,5%. Obrazloženja koja su ispitanici dali su slijedeća: „Jedini razlog za zabrinutost bi bila zaštita privatnosti. Ako bi se Internet stvari koristio stvarno samo za ono za što je namijenjen, ne bi bilo razloga za zabrinutost“, „Ne treba sve prepustiti strojevima, ljudska interpretacija informacija je i dalje nužna za većinu svakodnevnih aktivnosti“, „Svi ti uređaji su podložni hakerskim napadima ako nisu na kvalitetan način zaštićeni, isto kako netko vam može hakirati kameru na laptopu, tako može i sigurnosne kamere u kući recimo“, „Prvenstveno sto se osobni podatci mogu hakirati i zloupotrijebiti. Ujedno se čovjek zatupljuje

i manje pamti nego prije 10-15 god kad je tehnologija bila dosta manje razvijena“. Kao što se vidi iz priloženih komentara, mnogo zabrinutosti ispitanika oko razvoja Interneta stvari je oko sigurnosti takvih sustava. Jako malo ispitanika je navelo privatnost i zaštitu iste kao problem Interneta stvari, većina ih se više brine zbog sigurnosti osobnih stvari koje bi napadači mogli otuđiti. Usporedimo li rezultate ove ankete sa anketom koju je proveo MEF, vidimo da i naši građani dijele iste zabrinutosti kao i ispitanici razvijenijih zemalja.

6. Zaključak

Internet stvari pruža mnoge pogodnosti, od pametne kuće, pametnog automobila pa do pametnog grada, sve može biti umreženo i olakšati većinu života ljudima. No to je nemoguće učiniti osim ako se ne oduzme dio privatnosti. Ljudima nije problem pružiti neke osobne informacije u svrhu poboljšanja života, no žele biti sigurni da te informacije neće se koristiti u druge svrhe. Problem predstavlja i ogromna količina podataka koje će umreženi uređaji prikupljati jer zakoni o privatnosti ne pokrivaju te podatke. Ljudi ne žele da se pravi profil o njima na osnovu njihova kretanja, druženja, kupovanja, putovanja pa čak i načina na koji voze i da se ti profili koriste u svrhu za koje nisu ni svjesni poput procjenjivanja tržišta. Ljudi žele da imaju svoju privatnost, ali i da im život bude kao iz znanstveno-fantastičnih filmova gdje im je dom uvijek odgovarajuće temperature, svijetlo se samo ugasi kad napuste prostoriju, pegla se isključi kad napuste dom i žele da njihov dom bude siguran od uljeza i lopova. Žele da mogu provjeriti da li je netko ušao u njihov dom dok su na odmoru na moru bez da moraju zvati susjede. Žele da policija bude obaviještena ukoliko im netko pokuša ući u kuću dok spavaju. Ali ne žele da ih netko nadgleda kroz kamere koje bi trebale služiti da ih štite od uljeza. Ne žele da netko dobije ključ od njihove kuće i da zna kad neće biti kod kuće. Žele biti sigurni da imaju svoju privatnost, ali trenutno na tržištu Interneta stvari pametne kuće ne ispunjavaju do kraja te uvjete. Treba napomenuti da većina proizvođača uređaja koji se spajaju su maleni 'igrači' na tržištu koji samo žele napredak tehnologije, no nemaju potrebne resurse da naprave tehnologiju koja će poboljšavati život i ujedno biti sigurna, zato veliki 'igrači' poput Googla preuzimaju inicijativu. Istraživanje je pokazalo da postoji veliki strah od Interneta stvari, ponajviše što se tiče privatnosti, no sigurnost uređaja se povećava svakim danom i samo je pitanje vremena kada će povjerenje ljudi dovoljno narasti da Internet stvari uzme zamah i olakša svima život.

Popis literature

[1] H. Sundmaeker, P. Guillemin, P. Friess i S. Woelfflé (2010.) „Vision and Challenges for Realising the Internet of Things“, Luxembourg, Publication Office of the European Union

[2] „Worldwide and Regional Internet of Things(IoT) 2014-2020 Forecast: A Virtous Circle of Proven Value and Demand“. Dostupno: https://www.business.att.com/content/article/IoT-worldwide_regional_2014-2020-forecast.pdf [pristupano 13.9.2018.]

[3] M. Weiser. „The Computer for the 21st Century“. Dostupno: https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf [pristupano 13.9.2018.]

[4] J. Carretero, J.D. Garcia, „The Internet of Things: connecting the world“. Dostupno: https://rd.springer.com/article/10.1007/s00779-013-0665-z [pristupano 13.9.2018.]

[5] M.Rouse, „Internet of things (IoT)“. Dostupno: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT [pristupano 13.9.2018.]

[6] K. Ashton. (2009. 22. lip) „That 'Internet of Things' Thing“, *RFID Journal*. Dostupno: http://www.rfidjournal.com/articles/view?4986 [pristupano 13.9.2018.]

[7] D. Gorodyansky (2015.) „Privacy and Security in the Internet Age“. Dostupno: https://www.wired.com/insights/2015/01/privacy-and-security-in-the-internet-age/ [pristupano 13.9.2018.]

[8] D.D. Drajić. „Uvod u IoT(Internet of Things)“. Beograd, Srbija, Akademska misao

[9] J.H. Wilson, S. Baiju i B. Whipple (2015.) „How People Are Actually Using the Internet of Things“. Dostupno: https://hbr.org/2015/10/how-people-are-actually-using-the-internet-of-things [pristupano 13.9.2018.]

[10] B. Buntz (2016. 18. svi). „The World's 5 Smartest Cities“. Dostupno: https://www.iotworldtoday.com/2016/05/18/world-s-5-smartest-cities/ [pristupano 13.9.2018.]

[11] VIA tech, „In-Vehicle Solutions“. Dostupno: https://www.viatech.com/en/solutions/smart-transportation/in-vehicle/?cn-reloaded=1 [pristupano 13.9.2018.]

[12] Smart Farms [na Internetu]. Dostupno: http://smart-farms.net/ [pristupano 13.9.2018.]

[13] Macadamiam, Offie Practicum. „Integration RFID, NFC, and mobile techology and the cloud. Dostupno: http://cdn.macadamian.com/wp-content/uploads/Case-Study-Office-Practicum.pdf [pristupano 13.9.2018.]

[14] European Commission (2018. 14. Velj). „eCall: Time saved = lives saved“. Dostupno: https://ec.europa.eu/digital-single-market/en/ecall-time-saved-lives-saved#Article [pristupano 13.9.2018.]

[15] D. J. Glancy (1995.). „Privacy and Intelligent Tranportation Techonology“. Dostupno: http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1183&context=chtlj [pristupano 13.9.2018.]

[16] D. Slama, F. Puhlmann, J. Morrish i R. M. Bhatnagar (2015.) „Enterprise IoT“. Sebastopol, California, SAD, O'Reilly Media

[17] A. Lopez (2018. 13. ožu) „Protecting Your Privacy in an IoT-Connected World“. Dostupno: https://www.iotforall.com/protecting-privacy-in-iot/ [pristupano 13.9.2018.]

[18] M. della Cava. „Privacy integral to future of the Internet of Things“. Dostupno: https://eu.usatoday.com/story/tech/2014/07/10/internet-of-things-privacy-summit/12496613/ [pristupano 13.9.2018.]

[19] P. Ragusa (2018. 11. srp) „Alarm.com launches homebuilder program“. Dostupno: http://www.securitysystemsnews.com/article/alarmcom-launches-homebuilder-program [pristupano 13.9.2018.]

[20] A.F. Westin (1967.) „Privacy and Freedom“. New York: Atheneum. Dostupno: http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr [pristupano 13.9.2018.]

[21] Bleustein (1964.) „Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, New York University Law Review. Dostupno http://courses.ischool.berkeley.edu/i205/s10/readings/week11/bloustein-privacy.pdf [pristupano 13.9.2018.]

[22] J. DeCew (2013.) „Privacy“, The Stanford Encyclopedia of Philosophy. Dostupno: https://plato.stanford.edu/entries/privacy/ [pristupano 13.9.2018.]

[23] Trend Micro (2018. 1. velj) „Data Privacy in the Age of IoT“. Dostupno: https://blog.trendmicro.com/data-privacy-age-iot/ [pristupano 13.9.2018.]

[24] M. Rouse, M. Bacon (2017.) „Security“. Dostupno: http://searchsecurity.techtarget.com/definition/security [pristupano 13.9.2018.]

[25] MEF (2016.) „The Impact of Trust on IoT“. Dostupno: https://mobileecosystemforum.com//wp-content/uploads/2016/04/IoT_Exec_Summary.pdf [pristupano 13.9.2018.]

[26] T. Simpson (2016.) „We Want to Embrace the IoT But Can We Trust It?“. Dostupno: https://now.avg.com/we-want-to-embrace-the-iot-but-can-we-trust-it/ [pristupano 13.9.2018.]

[27] A. Bradshaw „FTC Says Privacy Still Matters on 'Internet of Things'“, [Blog post] 2015. [na Internetu]. Dostupno: https://cdt.org/blog/ftc-says-privacy-still-matters-on-internet-of-things/ [pristupano 13.9.2018.]

[28] R. Kitchin (2016.) „Getting smarter about smart cities: Improving data privacy and data security, Dublin, Irska: Data Protection Unit, Department of the Taoiseach. Dostupno: https://www.taoiseach.gov.ie/eng/Publications/Publications_2016/Smart_Cities_Report_January_2016.pdf [pristupano 13.9.2018.]

[29] O. Vermesan, P. Friess. „Internet of Things – From Research and Innovation to Market Deployment“. Dostupno: http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf [pristupano 13.9.2018.]

[30] C. Moore (2015.) „Home Automation Benchmarking Results“. Dostupno: https://www.synack.com/2015/03/14/home-automation-benchmarking-results/ [pristupano 13.9.2018.]

Popis slika